FortiClient v5.0.10
Administration Guide

FortiClient v5.0.10 Administration Guide

January 29, 2015

04-5010-183401-20150129

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-11-02	Initial release.
2012-11-07	Updated scripts chapters. This document is now inclusive of both Windows and Mac OS X. It is important to note that not all features available for Windows are available for Mac OS X.
2012-11-15	Updated IPsec and SSL VPN chapter.
2012-11-22	Added note about FortiClient License for FortiAuthenticator.
2012-11-27	Updated script commands to match changes in the *FortiClient version 5.0 XML Reference*.
2013-01-09	Updated for FortiClient version 5.0.1. Removed XML chapter, see to the *FortiClient version 5.0 XML Reference* for more information. Removed FortiClient Tools chapter, see the *FortiClient version 5.0.1 Release Notes* for more information.
2013-04-05	Updated for FortiClient version 5.0.2. Added new chapter for SCCM 2012.
2013-04-29	Updated for FortiClient version 5.0.3.
2013-05-27	Fixed typographic error.
2013-06-12	Updated for FortiClient version 5.0.4.
2013-08-21	Updated for FortiClient version 5.0.5.
2013-09-05	Added Appendix A: Using the FortiClient API. This is an advanced feature.
2013-10-10	Updated for FortiClient version 5.0.6.
2013-11-28	Updated for FortiClient version 5.0.7.
2014-03-07	Updated for FortiClient version 5.0.8.
2014-03-20	Minor document update. Added note to clarify FortiClient logging to FortiAnalyzer.
2014-04-17	Updated for FortiClient version 5.0.9.
2015-01-29	Updated for FortiClient version 5.0.10.

Introduction

FortiClient has been completely re-designed for version 5.0. FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient version 5.0.

This document was written for FortiClient (Windows) v5.0.10. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0.10.

FortiClient features

The following table provides a feature comparison between the standalone client (free version) and the managed client (licensed version).

Table 1: FortiClient feature comparison

Standalone Client (Free Version)	Managed Client (Licensed Version)
Threat Protection • Real-time Antivirus Protection • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware)	**Threat Protection** • Real-time Antivirus Protection • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware) • Cloud Based Behavior Scanning
Web Content • Web Filtering • Search Engine Safe Search Bing and Yandex • YouTube Education Filter	**Web Content** • Web Filtering • Search Engine Safe Search Bing and Yandex • YouTube Education Filter
VPN • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Two-Factor Authentication	**VPN** • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Two-Factor Authentication
Logging • VPN, Antivirus, Parental Control, and Update Logging • View logs locally	**Logging** • VPN, Application Firewall, Antivirus, Web Filter, Update, and Vulnerability Scan Logging • View logs locally

Table 1: FortiClient feature comparison (continued)

Standalone Client (Free Version)	Managed Client (Licensed Version)
	Application Control • Application Firewall • Block Specific Application Traffic
	Vulnerability Management • Vulnerability Scan • Link to FortiGuard with information on the impact and recommended actions
	Central Management • Centralized Client Management and monitoring • Centralized configuration provisioning and deployment • Enforcement of enterprise security policies.
	Central Logging • Upload logs to a FortiAnalyzer or FortiManager. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.

Licensing

Licensing on the FortiGate is based on the number of registered clients. FortiGate 30D series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, an upgraded license must be purchased. The maximum number of managed clients varies per device model.

Client limits

In high availability (HA) configurations, all cluster members require an upgrade license key. The following table shows client limits per FortiGate model series:

Table 2: FortiClient license upgrade

FortiGate Series	Free registrations	FortiClient license upgrade SKU
FortiGate/FortiWiFi 30 and 40 series	10	No upgrade license.
FortiGate/FortiWiFi 60 to 90 series	10	200 client registrations FCC-C0102-LIC
FortiGate 100 to 800 series and VM01 to VM02	10	2000 client registrations FCC-C0103-LIC
FortiGate 1000 to 5000 series and VM04 to VM08	10	8000 client registrations FCC-C0105-LIC

Installation information

The following table lists operating system support and the minimum system requirements.

Table 3: Installation information

Operating System Support	Minimum System Requirements
Microsoft Windows XP (32-bit) Microsoft Windows Vista (32-bit and 64-bit) Microsoft Windows 7 (32-bit and 64-bit) Microsoft Windows 8 (32-bit and 64-bit) Microsoft Windows 8.1 (32-bit and 64-bit)	Microsoft Internet Explorer version 8 or later Microsoft Windows compatible computer with Intel processor or equivalent Compatible operating system and minimum 512MB RAM 600MB free hard disk space Native Microsoft TCP/IP communication protocol Native Microsoft PPP dialer for dial-up connections Ethernet NIC for network connections Wireless adapter for wireless network connections Adobe Acrobat Reader for documentation MSI installer 3.0 or later.
Mac OS X v10.8 Mountain Lion Mac OS X v10.9 Mavericks Mac OS X v10.10 Yosemite	Apple Mac computer with an Intel processor 256MB of RAM 20MB of hard disk drive (HDD) space TCP/IP communication protocol Ethernet NIC for network connections Wireless adapter for wireless network connections

Language support

The following table lists FortiClient language support information.

Table 4: Language support

Language	Graphical User Interface	XML Configuration	Documentation
English (United States)	✔	✔	✔
Chinese (Simplified)	✔	-	-
Chinese (Traditional)	✔	-	-
French (France)	✔	-	-
German	✔	-	-

Table 4: Language support (continued)

Language	Graphical User Interface	XML Configuration	Documentation
Japanese	✔	-	-
Korean	✔	-	-
Portuguese (Brazil)	✔	-	-
Spanish (Spain)	✔	-	-

Please review the *FortiClient v5.0.10 (Windows) Release Notes* or the *FortiClient v5.0.10 (Mac OS X) Release Notes* prior to upgrading. Release Notes are available at the Customer Service & Support portal.

FortiClient language is dependent on the regional settings on the client workstation. When the regional language setting is not supported, FortiClient defaults to English.

What's New in FortiClient version 5.0

Summary of enhancements

This document was written for FortiClient (Windows) v5.0.10. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0.10.

FortiClient (Windows)

The following is a list of enhancements in FortiClient (Windows) version5.0.

FortiClient (Windows) version 5.0.10

- FortiClient can now run in Federal Information Processing Standard (FIPS) mode. It is certified to FIPS 140-2 Level 1 and Level 2. For reference, please see:

  NIST Computer Security Publications

  FIPS (Federal Information Processing Standards)

  http://csrc.nist.gov/publications/PubsFIPS.html
- The OpenSSL library has been updated to the latest version 1.0.1k.

FortiClient (Windows) version 5.0.9

- The OpenSSL library has been updated to the latest version 1.0.1g.

FortiClient (Windows) version 5.0.8

- There are no new features or enhancements in this release

FortiClient (Windows) version 5.0.7

- Improved antivirus scanning performance
- Improvements to the Endpoint Control GUI

FortiClient (Windows) version 5.0.6

- Improved usability of the repackager tool
- Repackaged clients can be upgraded
- Option to drop IPv6 traffic when an IPsec VPN connection is established. IPv4 traffic is sent through the tunnel or otherwise, depending on whether split tunnel is used.

FortiClient (Windows) version 5.0.5

- Enhanced file copy performance
- Customized installation: Users may choose to install the entire FortiClient feature set or only the VPN features. For more information, see "Custom FortiClient Installations" on page 109.
- Scan for viruses and malware on the target system before installing FortiClient
- Enhanced GUI performance

FortiClient (Windows) version 5.0.4

- Assign endpoint control profiles based on Active Directory group
  Requires a FortiGate running FortiOS version 5.0.3 or later.

  On a system using Active Directory (AD) for user account verification, FortiClient will send the AD user name and group to the FortiGate during Endpoint Control (EC) registration. The FortiGate may be configured to select the correct EC profile by user or group.
- Display endpoint control profile details in registration dialog box
  Requires a FortiGate running FortiOS version 5.0.3 or later.
- Removed Vulnerability Scan (VCM) and Application Firewall for standalone users
  Requires a FortiGate running FortiOS version 5.0.2 or later.

  FortiGate administrators may choose to display these two features (on FortiClient) for users registered to the FortiGate.
- Enhanced how the list and status of FortiGates are displayed for endpoint control registration

FortiClient (Windows) version 5.0.3

- Enhancements to FortiProxy
- Improved VPN usability with FortiToken

FortiClient (Windows) version 5.0.2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways

  Enables roaming clients
- Enhancement to the remembered FortiGates feature
- FortiClient uploads traffic, event, and vulnerability scan logs to FortiAnalyzer/FortiManager

  Requires a FortiAnalyzer/FortiManager device running version 5.0.2 or later and a FortiGate device running version 5.0.2 or later. In this release FortiClient logs are stored only. Support to view logs and create reports based on FortiClient logs will be added in a future release. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.
- SSL VPN realm support (command line only)
- Updated the OpenSSL library to version 1.0.1e
- Synchronize VPN elements; *save password*, *auto connect*, and *always up*; with the FortiGate
  Requires a FortiGate running FortiOS version 5.0.2 or later.
- Web category filtering safe search support

  For popular search sites or portals including Bing and Yandex.

FortiClient (Windows) version 5.0.1

- Endpoint Control registration over SSL VPN or IPsec VPN
- Remember multiple FortiGates for Endpoint Control registrations
- FortiClient console improvements

FortiClient (Windows) version 5.0.0

- Antivirus and Antimalware

  Protection against the latest virus, grayware (adware/riskware) threats.

  Client antivirus is free, and auto updates every three hours.
- Application firewall

  Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)

- Diagnostic tool
- Enhancements to the FortiClient console
- Endpoint Management using FortiGate, including:
  Automatic endpoint registration. User initiated endpoint registration.
  Deploy VPN (IPsec/SSL) configuration
  Enable or disable antivirus real-time protection.
  Manage and deploy web filtering and application firewall configuration.
- Localization support
- Parental Control/Web Filter
  Block, allow, warn, and monitor web traffic based on category.
- Remote Access (IPsec and SSL VPN)
  Secure Virtual Private Network access to your network.
  Supports multiple gateways for a single tunnel.
- Rootkit detection and removal
- Single Sign-On Mobility agent support with FortiAuthenticator/FSSO collector agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray
- VPN auto connect/always up
  Support the ability to automatically connect to a VPN tunnel without user interaction
  Support the ability to configure the VPN to always be connected
- Vulnerability scan
  Identify system and application vulnerabilities.

FortiClient (Mac OS X)

The following is a list of enhancements in FortiClient (Mac OS X) version 5.0.

FortiClient (Windows) version 5.0.10

- Added support for Mac OS X 10.10 (Yosemite)
- The OpenSSL library has been updated to the latest version 1.0.1k.

FortiClient (Mac OS X) version 5.0.9

- There are no new features or enhancements in this release

FortiClient (Mac OS X) version 5.0.8

- There are no new features or enhancements in this release

FortiClient (Mac OS X) version 5.0.7

- Improvements to the Endpoint Control GUI

FortiClient (Mac OS X) version 5.0.6

- Option to drop IPv6 traffic when an IPsec VPN connection is established. IPv4 traffic is sent through the tunnel or otherwise, depending on whether split tunnel is used.

FortiClient (Mac OS X) version 5.0.5

- Customized installation: Users may choose to install the entire FortiClient feature set, or just the VPN. For more information, see "Custom FortiClient Installations" on page 109.

FortiClient (Mac OS X) version 5.0.4

- Assign endpoint control profiles based on Active Directory group
  Requires a FortiGate running FortiOS version 5.0.3 or later

  On a system using Active Directory (AD) for user account verification, FortiClient will send the AD user name and group to the FortiGate during endpoint control (EC) registration. The FortiGate may be configured to select the correct EC profile by user or group.
- Display endpoint control profile details in registration dialog box
  Requires a FortiGate running FortiOS version 5.0.3 or later
- Removed Vulnerability Scan (VCM) and Application Firewall for standalone users

  FortiGate administrators may choose to display these two features (on FortiClient) for users registered to the FortiGate.
- Enhanced how the list and status of FortiGates are displayed for Endpoint Control registration

FortiClient (Mac OS X) version 5.0.3

- Improved VPN usability with FortiToken

FortiClient (Mac OS X) version 5.0.2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways (maximum 20)

  Enables roaming clients.
- Enhancements to the remembered FortiGates feature
- FortiClient uploads traffic and vulnerability scan logs to FortiAnalyzer/FortiManager

  Requires a FortiAnalyzer/FortiManager device running version 5.0.2 or later and a FortiGate device running version 5.0.2 or later. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.
- FortiClient console improvements
- FortiClient traffic logging
- Improved VPN controller reliability
- Silent registration element added to the `endpoint_control` section in the XML configuration file.
- Synchronize VPN elements; `save password`, `auto connect`, and `always up`; with the FortiGate.
  Requires a FortiGate running FortiOS version 5.0.2 or later.
- Web category filtering safe search support

  For popular search sites or portals including: Bing and Yandex.

FortiClient (Mac OS X) version 5.0.1

- Remember multiple FortiGates for Endpoint Control registrations
- Endpoint Control registration over SSL VPN and IPsec VPN
- Improvements to the FortiClient GUI
- Splash screen
- VPN resiliency

FortiClient (Mac OS X) version 5.0.0

- AntiVirus and Antimalware
  Protection against the latest virus, grayware (adware/riskware) threats.
  Client antivirus is free, and auto updates every three hours.
- Application Firewall
  Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)
- Diagnostic Tool
- Enhancements to the FortiClient dashboard
- Endpoint Management using FortiGate, including:
  Automatic endpoint registration. User initiated endpoint registration.
  Deploy VPN (IPsec/SSL) configuration
  Enable or disable AntiVirus real-time protection.
  Manage and deploy Web Filtering and Application Firewall configuration.
- Localization support
- Parental Control/Web Filter
  Block, allow, warn, and monitor web traffic based on category.
- Remote Access (IPsec and SSL VPN)
  Secure Virtual Private Network access to your network.
  Supports multiple gateways for a single tunnel.
- Single Sign-On Mobility Agent support with FortiAuthenticator/FSSO Collector Agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray
- VPN auto connect/always up
  Support the ability to automatically connect to a VPN tunnel without user interaction
  Support the ability to configure the VPN to always be connected
- Vulnerability Scan
  Identify system and application vulnerabilities.

Provisioning FortiClient

FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems using Microsoft Active Directory (AD) or the Microsoft System Center 2012 Configuration Manager (SCCM).

This chapter contains the following sections:

Standard FortiClient installation

The following section describes installing FortiClient to a standalone Microsoft Windows and Apple Mac computer.

Download the FortiClient installation files

The FortiClient installation files can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

  Requires a support account with a valid support contract. Download either the Microsoft Windows (32-bit/64-bit) or the Mac OS X online installation file.
- FortiClient homepage: www.forticlient.com

  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.
- Fortinet Resource Center: http://www.fortinet.com/resource_center/product_downloads.html

  Download the FortiClient online installation file. On this page you can download the latest version of FortiClient for Microsoft Windows, Mac OS X, iOS, and Android.

In FortiOS v5.0.1 or later, you can download the FortiClient installation files in the FortiGate dashboard. Go to *System* > *Dashboard* > *Status,* in the *License Information* widget, select *Mac* or *Windows* to download the FortiClient Online Installer file.

Install FortiClient on a Microsoft Windows computer

The following instructions will guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) v5.0.10 Release Notes*.

When installing FortiClient version 5.0.5 or later, it is recommended to use the FortiClient Online Installer file. This file will launch the FortiClient Virus Cleaner which will scan the target system prior to installing the FortiClient application.

To check the digital signature of FortiClient, right-click on the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.

To install FortiClient (Windows):

1. Double-click the FortiClient executable file to launch the setup wizard. The *Setup Wizard* will launch on your computer. When using the FortiClient Online Installer file, the FortiClient Virus Cleaner will run before launching the *Setup Wizard*. If a virus is found that prevents the infected system from downloading the new FortiClient package, see "Installing FortiClient on an infected system" on page 19.

   The *Welcome* screen appears.
2. Read the license agreement and select *Next* to continue. You have the option to print the EULA in this window.
3. Select *Change* to choose an alternate folder destination for installation. Select *Next* to continue.
4. FortiClient will search the target system for other installed antivirus software. If found, FortiClient will display the *Conflicting Antivirus Software* page. You can either exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient real-time protection disabled.

This dialog box is displayed during a new installation of FortiClient and when upgrading from an older version of FortiClient which does not have the antivirus feature installed.

It is recommended to uninstall the conflicting antivirus software before installing FortiClient or enabling the antivirus real-time protection feature. Alternatively, you can disable the antivirus feature of the conflicting software.

5. Select Next to continue.
6. Select *Install* to begin the installation.
7. Select *Finish* to exit the FortiClient Setup Wizard.
8. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now, or select *No* to manually restart later.
9. To launch FortiClient, double-click the desktop shortcut icon.

Install FortiClient on a Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the *FortiClient (Mac OS X) v5.0.10 Release Notes.*

To install FortiClient (Mac OS X):

1. Double-click the FortiClient `.dmg` installer file to launch the FortiClient installer. The *FortiClient Installer* will install FortiClient on your computer. Select *Continue*.

   Select the lock icon in the upper right corner to view certificate details.
2. Read the Software License Agreement and select *Continue*. You have the option to print or save the Software Agreement in this window. You will be prompted to *Agree* with the terms of the license agreement.
3. Select the destination folder for the installation.

4. Select *Install* to perform a standard installation on this computer. You can change the install location from this screen.
5. Depending on your system, you may be prompted to enter your system password.
6. The installation was successful. Select *Close* to exit the installer.
7. FortiClient has been saved to the *Applications* folder.
8. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon in the FortiClient console to make changes to the FortiClient configuration.

Installing FortiClient on an infected system

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading of the new FortiClient package, use the following process:

- Boot into “safe mode with networking” (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network).
- Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs subdirectory. If a virus is found, it will be quarantined. When complete, reboot back into normal mode and run the FortiClient installer to complete the installation.

Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message will be generated. It is necessary to reboot back into normal mode to complete the installation.

Installing FortiClient as part of a cloned disk image

If you configure computers using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image:

1. Using an MSI FortiClient installer, install and configure the FortiClient application to suit your requirements.

   You can use a standard or a customized installation package.
2. Right-click the FortiClient icon in the system tray and select Shutdown FortiClient.

3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on.

5. Create the hard disk image and deploy it as needed.

Installing FortiClient on cloned computers

If you intend to create an image of the hard drive for deployment to other computers, you need to shut down FortiClient and use the RemoveFCTID tool to remove the FortiClient identifier.

Deploy FortiClient using Microsoft Active Directory (AD) server

There are multiple ways to deploy FortiClient to endpoint devices including using Microsoft Active Directory.

The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new Organizational Unit (OU).
7. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
8. Select *Start* > *Administrative Tools* > *Group Policy Managemen*t. The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and Link it here. Give the new GPO a name then select *OK*.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in will open.

10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
11. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package will then be generated.
12. If you wish to expedite the installation process, on both the server and client computers, force a GPO update.
13. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstall FortiClient using Microsoft Active Directory server:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* will open.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package that was used to install FortiClient.
3. Right-click the package, select *All Tasks* > *Remove*. Choose Immediately uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package will delete.
4. If you wish to expedite the uninstallation process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Deploy FortiClient using Microsoft SCCM 2012

The Microsoft System Center 2012 Configuration Manager (SCCM) may be used to deploy and manage multiple FortiClient Installations. This section presents various scenarios that you can utilize.

A fully functional SCCM server, along with discovered devices, is required. Visit the Microsoft web site for supporting documentation.

These instructions assume you have already installed and configured SCCM. If you have not, please refer to Microsoft's online help sources for information on this task.

The Microsoft *System Center 2012 Configuration Manager* (SCCM) may be used to deploy and manage multiple FortiClient Installations. This chapter presents various scenarios that you can utilize.

A fully functional SCCM server, along with discovered devices, is required. Visit the Microsoft web site for supporting documentation.

The following topics are detailed in this section:

- SCCM setup
- Task sequences
- Task sequence examples for FortiClient.

SCCM setup

Microsoft maintains a public free virtual lab of the *System Center 2012 Configuration Manager* (SCCM) at http://technet.microsoft.com/virtuallabs/bb539977.

At this page you can access a completely installed and properly configured system that can be used for testing various SCCM deployment scenarios. For ongoing enterprise use, a new system has to be created and configured.

SCCM product home page: http://www.microsoft.com/server-cloud/system-center

Technet documentation: http://technet.microsoft.com/systemcenter

Microsoft documentation: http://www.microsoft.com/en-ca/download/details.aspx?id=29901

The following subsections discuss some of the preparations required to enable control of FortiClient host computers.

Client discovery options and configuration

The *Configuration Manager* uses various methods to discover the Windows devices that an administrator can control on the network. One such method is the use of a common domain. To use this method, the Windows server hosting the *Configuration Manager* should be configured as domain controller. All Windows devices that will be managed should then join the domain. The *Configuration Manager* automatically discovers all Windows devices that join.

Client installation

The *Configuration Manager* console may be used to install configuration manager client software on target Windows devices that have joined the controlled domain. This is required for pushing the configuration to the devices.

Client policy polling interval settings

The configuration manager client on each Windows device polls for policy changes on the server at a regular interval. The polling interval defaults to 60 minutes. Each newly pushed or deployed task will run on all selected clients within this polling interval. You can customize the polling interval as required.

Client collections

New configurations are usually deployed to collections of devices. All of the devices that have joined the controlled domain will be added to a default collection.

You may want to deploy a different set of configurations to different groups of devices based on your user base. This can be accomplished by creating different client collections. Devices that have joined the domain will be added to one or more of those collections. Configurations may then be selectively deployed.

Client security issues

The *Configuration Manager* is able to deploy a large variety of applications to all the devices that joined the domain. Most of these tasks run with the administrator or system user authorisation level on the client devices. It is important to keep the *Configuration Manager* host under the highest level of security control possible.

It is also important to always test new planned application deployments in a controlled lab environment, or on a small client collection, before deploying to the entire client base.

Network share for all clients

The *Configuration Manager* console is used to deploy applications to client devices. Some of the applications require specification of files by file path and name. The client devices must have access to the files when the applications run. For instance, to upload a FortiClient XML configuration file to a given client collection, all client devices in the collection must independently have local access to the new XML configuration file.

The files may be provided by any suitable method. Examples include use of an HTTP or FTP server. The examples in this document use a network share. This should be available to all devices on the given client collection.

Task sequences

The *Configuration Manager* provides task sequences as a means of deploying commands to discovered clients without requiring user intervention. The FortiClient configuration examples in this chapter use the *Run Command Line* task sequences to run various command-line commands on client devices.

Task sequences are described in the following Microsoft documents:

Planning a Task Sequence Strategy

http://technet.microsoft.com/en-us/library/gg712685.aspx

How to Manage Task Sequences

http://technet.microsoft.com/en-us/library/hh273490.aspx

Here is a simple example of how task sequences may be used to control client devices.

In this example, a simple set of command-line commands are created in the *Configuration Manager* console. Once deployed, the commands will print information requested to the log file for each client.

The following commands will be executed on each client:

```
cd
dir c:\users
whoami
```

The first command will print the current working directory. This is likely to be `c:\windows\system32`. The second command will print the contents of the specified directory. The third command will print the name of the current user (the user under which the task sequence is running).

The output of the commands can be found in the log file on each client device at:

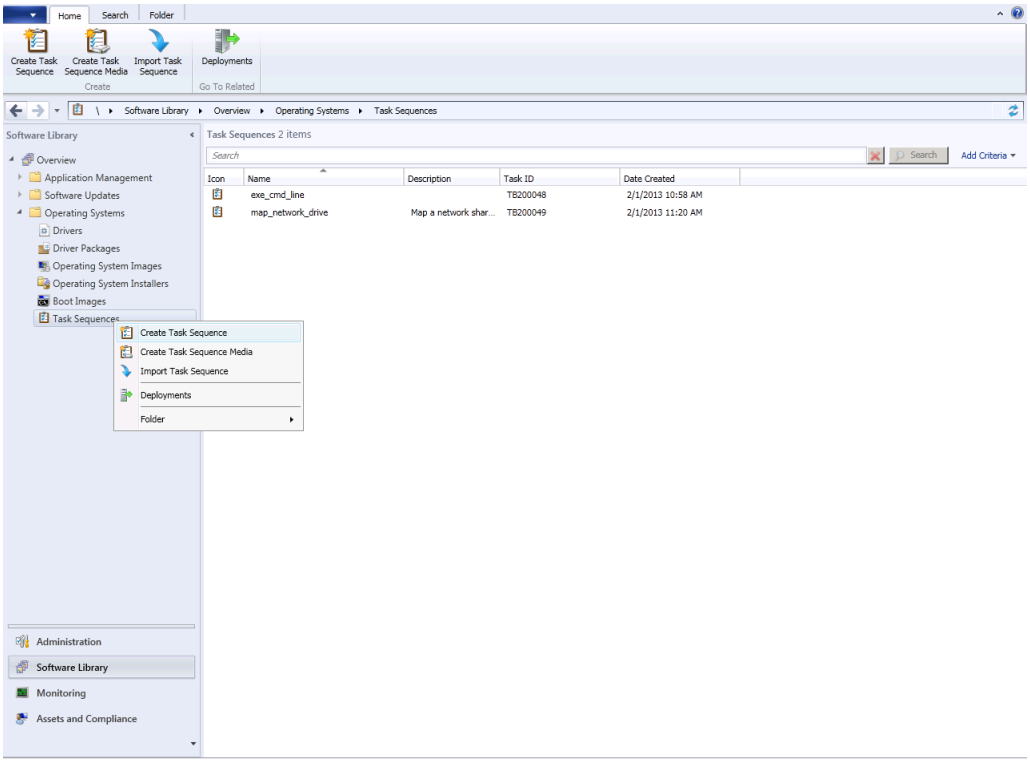
```
C:\Windows\CCM\Logs\smsts.log
```

To create a new task sequence:

1. Launch the *Configuration Manager* console.

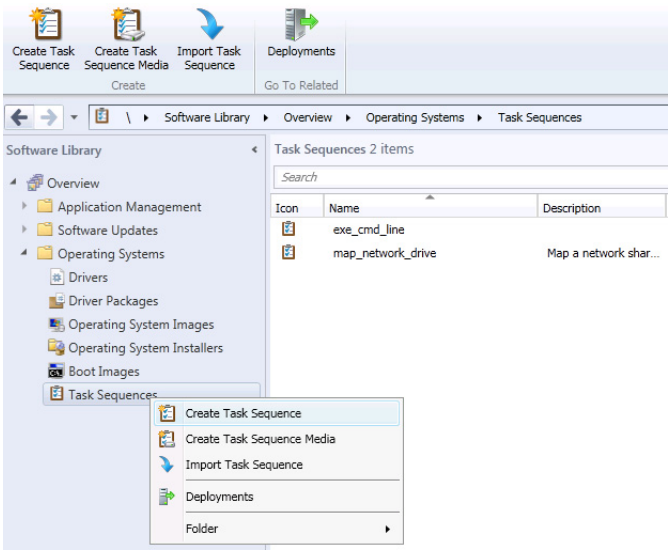
   The *Configuration Manager* console opens.

Figure 1: SCCM configuration manager



2. Select *Software Library* > *Overview* > *Operating Systems* > *Task Sequences.*
3. Right-click the *Task Sequence* menu item and select *Create Task Sequence.*

Figure 2: Right-click menu

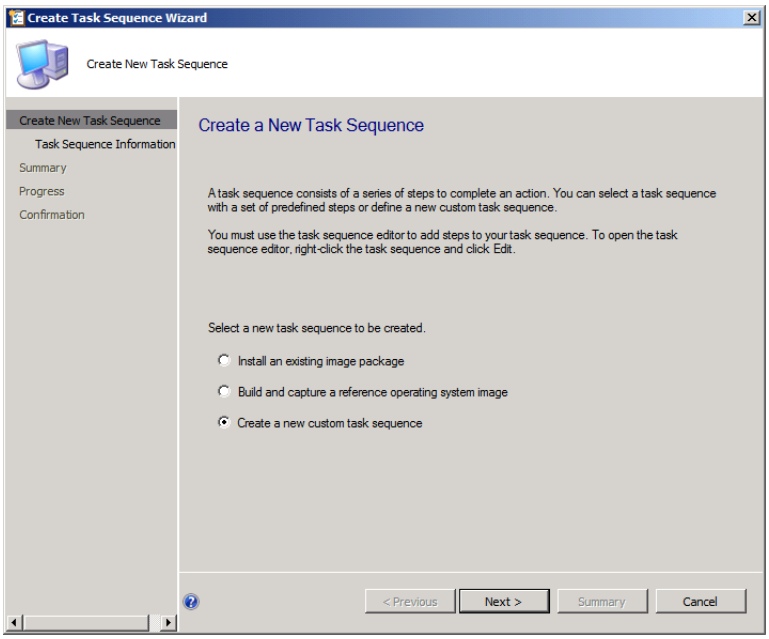


Alternatively, you can select *Create Task Sequence* in the toolbar.

Figure 3: Toolbar menu items

The *Create Task Sequence Wizard* opens.

Figure 4: Create task sequence task wizard



4. Select the *Create a new custom task sequence* radio button. Then select *Next* to proceed.
5. Enter a name for the task sequence.
6. Enter a comment to describe the task sequence.
7. Select *Next* to proceed.

   A summary of the task sequence configuration is displayed.
8. Select *Close* to save the configuration. The new task sequence is created and displayed in the *Configuration Manager* console.
9. Select *Task Sequences* in the menu in the left pane of the *Configuration Manager* console. The new task sequence is displayed in the right pane.

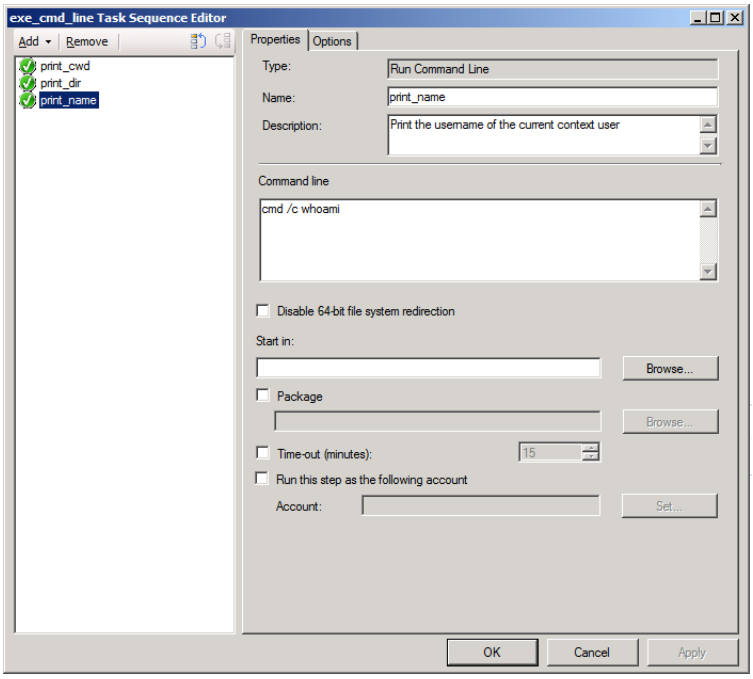
To add individual tasks into the task sequence:

1. Right-click in the newly created task sequence.
2. From the shortcut menu list, select *Edit*. The *Task Sequence Editor* dialog box is displayed.

   Alternatively, select the *Task Sequence* and select the *Edit* icon in the toolbar.
3. Select the *Add* drop-down button.
4. From the drop-down list, select *General* and the select *Run Command Line.*

   A new tab is displayed in the right pane of the dialog box.

Figure 5: Command line window



5. Configure the following settings:

Name	Enter a name for the command.
Description	Enter a description for the command.

Command line	Enter the command line in the text field.
	The command will usually start with “cmd /c”. For instance, the first command in this example is entered as:
	`cmd /c cd`
	`cmd /c dir c:\users`
	`cmd /c whoami`

6. Select *Apply* to apply the configuration.
7. Select OK to continue.

The task sequence will be saved with the three command-line tasks. To view or modify the tasks, select *Edit* in the short-cut menu for the selected task sequence.

There are three commands in this example. Each of the commands may be created as a single task. There will be a total of three tasks in the left pane of the dialog box. Each of the tasks will have one of the command-line commands:

```
cmd /c cd
cmd /c dir c:\users
cmd /c whoami
```

This format is preferred as it isolates any client errors to a specific task.

The three commands may also be combined into a lengthy single command:

```
cmd /c cd  ;  dir c:\users  ;  whoami
```

This format may mask task sequence errors. It is not recommended.

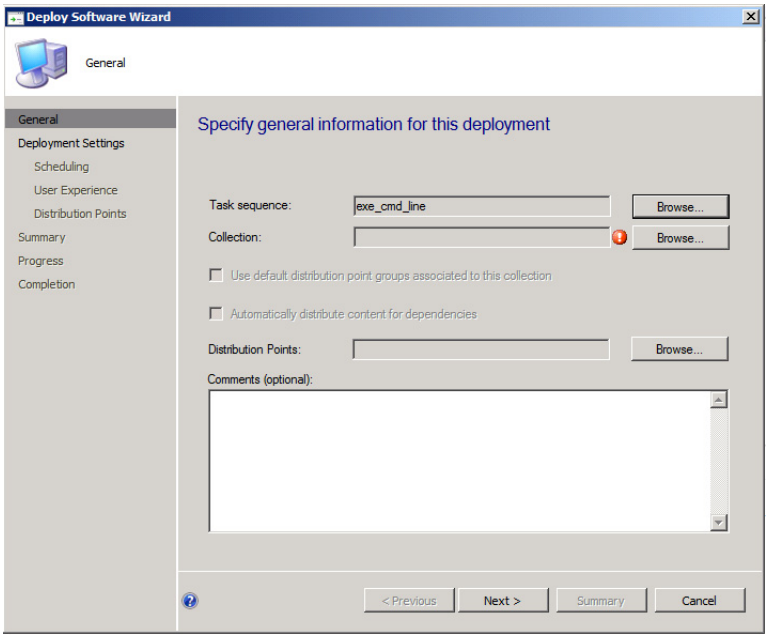
There is also an option to use a batch script.

Deploy the task sequence:

1. Right-click the task sequence.
2. Select *Deploy* in the right-click menu list.

   The *Deploy Software Wizard* dialog box opens.

   Figure 6: Deploy software wizard dialog box

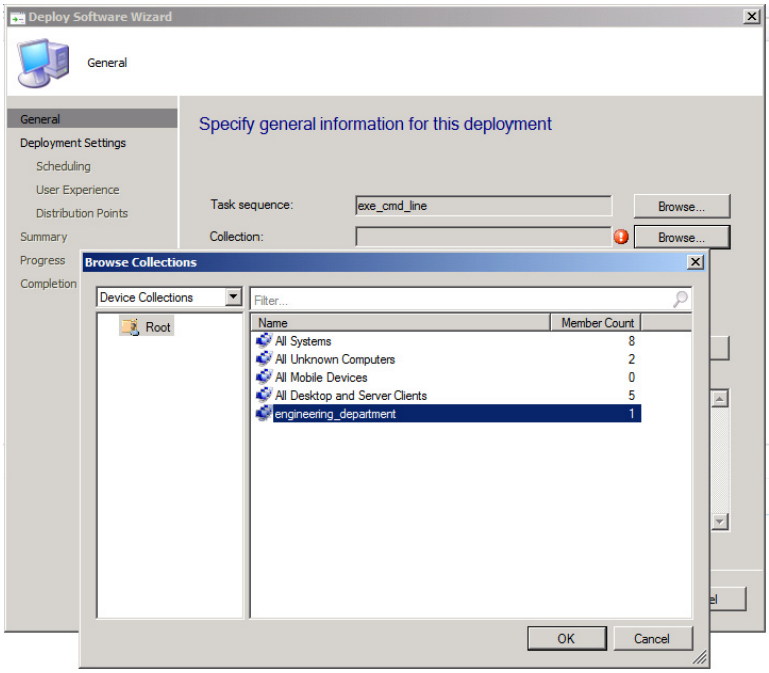


   Alternatively, select the *Task Sequence* and select the *Deploy* icon in the toolbar.

3. Select *Browse*.

   A *Browse Collections* dialog box appears listing all currently configured client collections.

Figure 7: Browse collections dialog box



4. Select the client collection to which this task sequence should be deployed
5. Select *OK* to close the *Browse Collections* dialog box. Pressing CTRL returns you to the *General* tab of the *Deploy Software Wizard* dialog box.
6. Select *Next*. The *Deployment Settings* tab is displayed
7. In the *Purpose* drop-down menu select *Required*. This makes the task mandatory for all clients receiving it.
8. Select the *Send wake-up packets* checkbox to enable this feature.
9. Select *Next*. The *Scheduling* tab is displayed
10. Select *New*. In the *Assignment Schedule* dialog box select the *Assign immediately after this event* radio button.
11. Select *OK*. This closes the *Assignment Schedule* dialog box. The *Scheduling* tab is displayed.
12. Select *Next*. The *User Experience* tab is displayed.
13. Select the *Show Task Sequence progress* checkbox to enable this feature.

    This configuration is optional. It displays a progress dialog box on each client as the task executes. If a silent background execution of tasks is desired, leave this checkbox unchecked.
14. Select *Next*. The *Distribution Points* tab is displayed. For this example, there is nothing to change in this tab.
15. Select *Next*. The *Summary* tab is displayed.
16. Select *Next*. The *Completion* tab is displayed which shows a summary of all selections.
17. Select *Close* to close the *Deploy Software Wizard*.

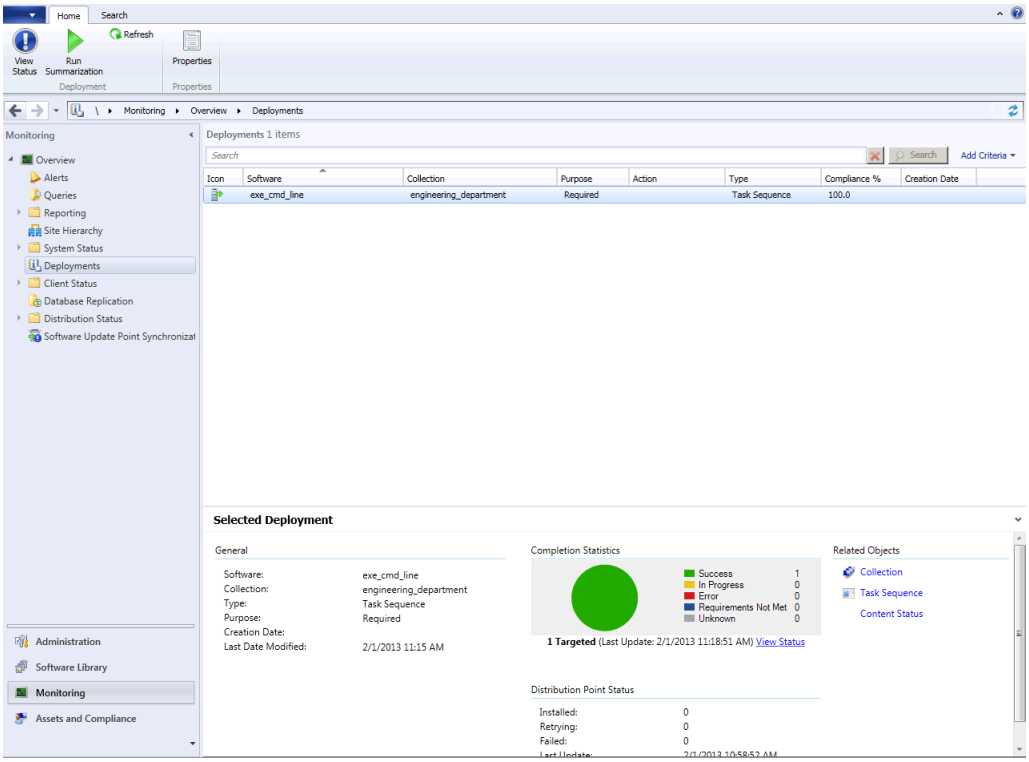
This completes the deployment of the task sequence to the selected client collections. Client devices in the collection should start to receive and execute the task. All clients will run the task within the *Policy Polling Interval* configured.

Monitor a deployed task sequence:

1. Launch the *Configuration Manager* console.
2. Select *Monitoring* from the tree-menu.
3. Select the *Overview* menu item in the left pane to expand the menu.
4. Select the *Deployments* menu item. The list of deployments is displayed in the right pane.
5. Click to select the recently deployed task sequence in the right pane.

   The *Deployments* window is displayed.

Figure 8: .Deployment window



To monitor a deployed task sequence on the client device, use the following process:

1. Launch the *Software Center* console on the client device. It displays a list of tasks deployed to it.

If a recently deployed task sequence is not displayed, most likely the *Policy Polling Interval* is yet to expire on this client.

2. Select the *Task Sequence*. The current status is displayed.

In addition to the two monitoring procedures above, the client log file is available on the client device at:

```
C:\Windows\CCM\Logs\smsts.log
```

It will contain details of the task sequence, including:

- the command-line commands executed
- any output generated by the commands
- any error messages

Mapping a network drive

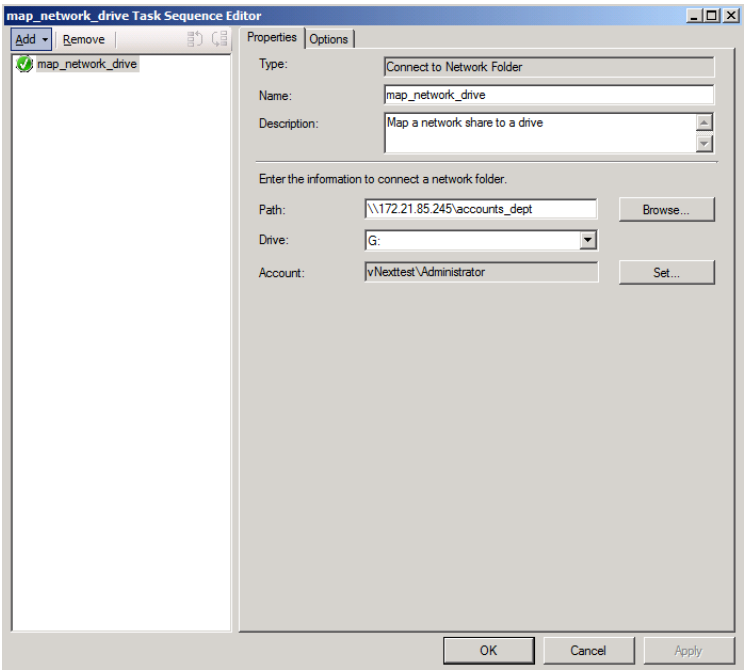
When a file is referenced in a task sequence, it must be made available to all clients before the task sequence starts. The processes listed below explain how to map a network folder to a drive in a given task sequence. If the mapping is successful, all the files in the shared folder will be available for the command-line commands in the task sequence.

To map a network drive in the task sequence:

1. Create a new custom task sequence.
2. Edit the task sequence.

   The *Task Sequence Editor* dialog box is displayed.

   Figure 9: Task sequence editor dialog box



3. Select the *Add* drop-down button.
4. In the drop-down list, select *General* > *Connect to Network Folder*. A new tab is displayed in the right pane of the dialog box.
5. Type a name for the command.
6. Type a description for the command.
7. Type the full path to the network shared folder or use the *Browse* button to select it.

When using the *Browse* button, be sure that the network share is being reported with the same path as the client devices will use.

Here is an example of a valid path: \\172.21.85.245\accounts_dept

8. Type a drive letter, along with a colon.

   For example: G:

9. Select *Set* and provide a user name and password that is valid for the network shared folder selected.
10. Select *OK* to return to the *Task Sequence Editor* dialog box.
11. Select *Apply* to save the task.

More tasks may be added to the task sequence as described in earlier parts of this section. Tasks may be re-ordered using the other buttons provided in the top of the left pane in the *Task Sequence Editor* dialog box.

When all tasks have been added, select *OK* to close the dialog box.

Task sequence examples for FortiClient

The task sequence processes described in the preceding section may be applied to any regular Windows tasks that runs on the command line. This section discusses several example FortiClient configurations that could be completed from the Windows command-line.

The examples in this section list only the command-line commands to be used. When deploying these from the *Configuration Manager* console, remember to always use the processes discussed this chapter to create the task sequence. The procedure is the same, only the contents of the *Run Command Line* commands will differ.

Install FortiClient

FortiClient can be installed from the command line using `msiexec`. In this example, a FortiClient MSI file that is provided on a network shared folder is used to install FortiClient to devices in the client collection.

Use the following commands in a task sequence to install FortiClient on a Windows client device.

1. Connect to a network folder:
   - Name: `map_network_drive`
   - Description: Mount a network shared directory that contains the FortiClient image to install
   - Path: \\172.21.85.245\accounts_dept
   - Drive: G:
   - Account: `vNexttest\administrator`
2. Run command line:
   - Name: `copy_fct_image`
   - Description: Copy FortiClient MSI image from network shared directory
   - Command line: `cmd /c copy /y G:\FortiClient.msi c:\temp\FortiClient.msi`
3. Run command line:
   - Name: `install_fct`
   - Description: Install FortiClient using MSI image
   - Command line: `cmd /c msiexec /i c:\temp\FortiClient.msi /qn`

Ensure that the FortiClient.msi file is available in the network share, and that the network share is accessible to all client devices in the client collection before deploying this task sequence.

Export the FortiClient XML configuration file

FortiClient features may be controlled using an XML configuration file. The configuration file is first exported from FortiClient, modified with a text editor, and re-imported into FortiClient. The XML configuration syntax and usage is documented in the *FortiClient v5.0.10 XML Reference*.

Use the following commands in a task sequence to export the XML configuration file from a Windows client device which has FortiClient installed.

1. Connect to a network folder:
   - Name: map_network_share
   - Description: Mount a network shared directory to which configuration file will be copied.
   - Path: \\172.21.85.245\engineering_dept
   - Drive: M:
   - Account: vNexttest\administrator
2. Run command line:
   - Name: export_fct_xml
   - Description: Export the FortiClient XML configuration file
   - Command line: cmd /c C:\Program Files\Fortinet\FortiClient\fcconfig -o export -f c:\temp\fct_xml.conf
3. Run command line:
   - Name: copy_fct_xml
   - Description: Copy FortiClient XML file to network shared directory
   - Command line: cmd /c copy /y c:\temp\fct_xml.conf M:\

This copies fct_xml.conf to the mounted share. If there is more than one device in the client collection, they will each overwrite the same file. You may use a batch script to uniquely rename the file as it is copied.

The full path to the FortiClient installation directory is used as a prefix to FCConfig.exe. The value provided in this example is the default on a 32-bit system. The default on 64-bit systems is:

```
C:\Program Files (x86)\Fortinet\FortiClient
```

If the client collection has a mixture of both 32-bit and 64-bit devices, a batch script may be used to selectively run from the correct platform-dependent directory.

Import a modified XML configuration file

Use the following commands in a task sequence to import an XML configuration file into FortiClient in a Windows client device.

1. Connect to a network folder:

   Name: map_network_share

   Description: Mount a network shared directory that contains the XML configuration file

   Path: \\172.21.85.245\engineering_dept

   Drive: M:

   Account: vNexttest\administrator

2. Run command line:

   Name: copy_fct_xml

   Description: Copy FortiClient XML configuration file from network shared directory

   Command line: cmd / c copy /y M:\fct_xml.conf c:\temp\

3. Run command line:

   Name: import_fct_xml

   Description: Import the FortiClient XML configuration file

   Command line: cmd /c “C:\Program Files\Fortinet\FortiClient\fcconfig -o import -f c:\temp\fct_xml.conf”

The same configuration file is used by all devices in the client collection.

When deploying a custom FortiClient XML configuration, use the advanced Endpoint Profile options in FortiGate to ensure the Endpoint Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Upgrade FortiClient

The FortiClient upgrade process is similar to the regular installation. The only difference is the use of a different version of FortiClient during the installation. A reboot is required, but the task sequence should handle this properly.

The same procedure listed earlier for FortiClient installation could be reused.

Uninstall FortiClient

Use the following command in a task sequence to uninstall FortiClient from Windows client devices.

1. Run command line:
   - Name: uninstall_fct
   - Description: Uninstall FortiClient
   - Command line: wmic product where name="FortiClient" call uninstall /nointeractive

The task sequence should process the required reboot correctly.

Endpoint Management

Introduction

The purpose of this section is to provide basic instructions on how to configure, deploy, and manage FortiClient configurations from your FortiGate device.

Endpoint Management requires FortiClient version 5.0.0 or later and a FortiGate device running FortiOS version 5.0.0 or later, or a FortiCarrier device running FortiOS Carrier version 5.0.0 or later. Certain features are only available on version 5.0.2 or later.

Endpoint Management is available on FG-30D model series and higher.

Configure endpoint management

In FortiOS version 5.0, configuration and management of FortiClient endpoint agents are handled by FortiGate. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured FortiClient profile to connected devices. The FortiClient profile can be deployed to devices on your network and over a VPN connection. You can configure multiple FortiClient profiles. The FortiClient profile consists of the following sections:

- Antivirus Protection
- Web Category Filtering

  You can select the web filtering profile to associate with the FortiClient profile. You can also select to disable Web Category Filtering when the client is protected by the FortiGate.
- VPN

  Select to enable client VPN provisioning. You can specify the VPN name, type, gateway and other settings the client will use to connect to your FortiGate device via the VPN connection. Two-factor authentication is configured in the FortiGate VPN configuration.
- Application Firewall

  You can select the application control sensor to associate with the FortiClient profile.
- Endpoint Vulnerability on Client

  You can select to scan daily, weekly or monthly. You can also select to scan the client after registration with your FortiGate device.

- Upload logs to FortiAnalyzer/FortiManager

  You can select to use the same IP address as the FortiGate device or specify a different device IP address. You can specify the frequency of the log upload.

FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.

- Use FortiManager for client software/signature update

  Select to enable this feature and enter the IP address of your FortiManager device. You can select to failover over to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.
- Dashboard Banner

  You can select to display or hide the FortiClient advertisement banner.

  Select if profile details may be displayed before endpoint control registration is completed.

See the *FortiOS Handbook 5.0* for more information on configuring your FortiGate device.

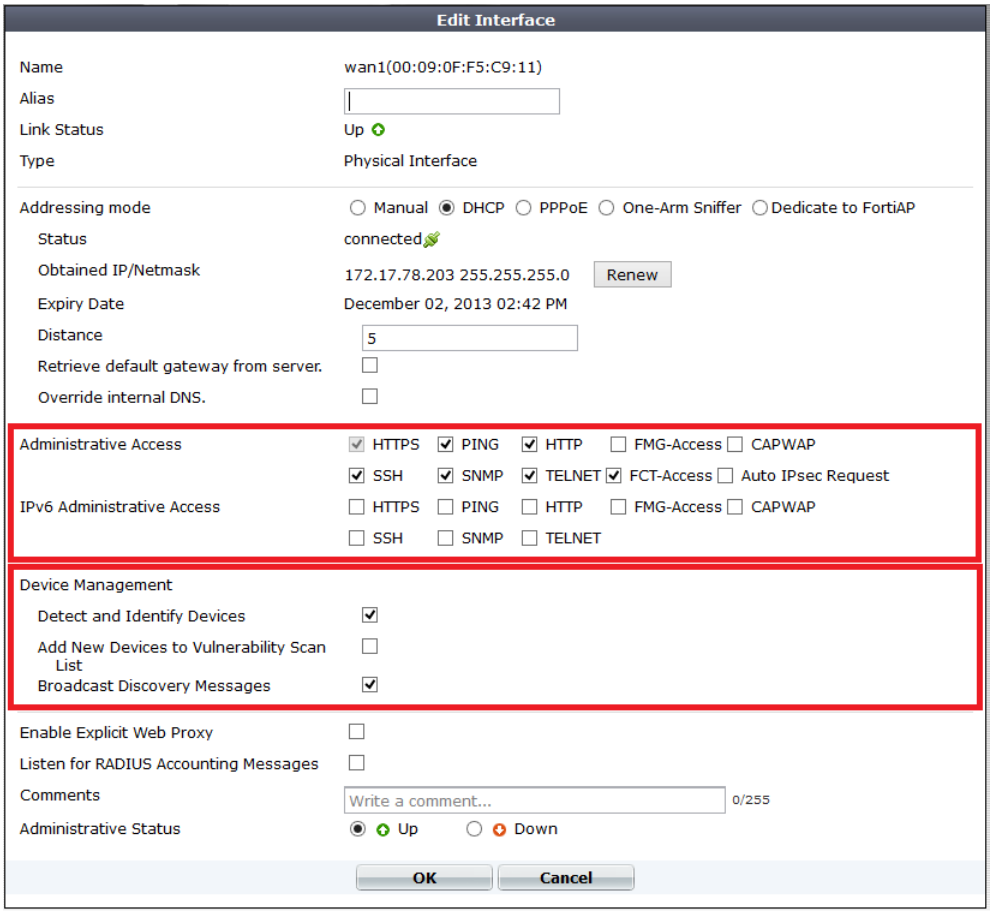
Configure Endpoint Management on the FortiGate device:

1. Enable device management and broadcast discovery messages.

   To configure *Device Management,* go to *System* > *Network* > *Interfaces,* select the applicable interface, and select *Edit* in the toolbar. In the *Edit Interface* page you can select to enable *Detect and Identify Devices.* To enable *Broadcast Discovery Messages* (optional) you must first enable *FCT-Access* under *Administrative Access*. Select *OK* to save the setting.

Broadcast Discovery Messages is an optional configuration. When enabled, the FortiGate will broadcast messages to your network, allowing client connections to discover the FortiGate for FortiClient registration. Without this feature enabled, the user will enter the IP address or URL of the FortiGate to complete registration.

Figure 10: Edit interface window



Configure the following settings:

Administrative Access	Select the checkbox for FCT-Access. This option is available for both IPv4 and IPv6 Administrative Access.
Security Mode	Select None or Captive Portal. When selecting Captive Portal, users are forwarded to a captive portal where they need to enter their username and password to authenticate with the FortiGate. You can customize the portal message and specify user groups. Note: This option is available when Addressing mode is set to Manual.
Device Management	
Detect and Identify Devices	Select to detect and identify devices on the selected interface.

Add New Devices to Vulnerability Scan List	As devices are found, they are added to the Asset Definitions list of the Vulnerability scanner. You can choose to run a scan of all of the devices on the list or of selected items, including devices found using FortiGate device identification.
Broadcast Discovery Messages	Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message.

Figure 11: Example captive portal replacement message

Configure the FortiClient profile:

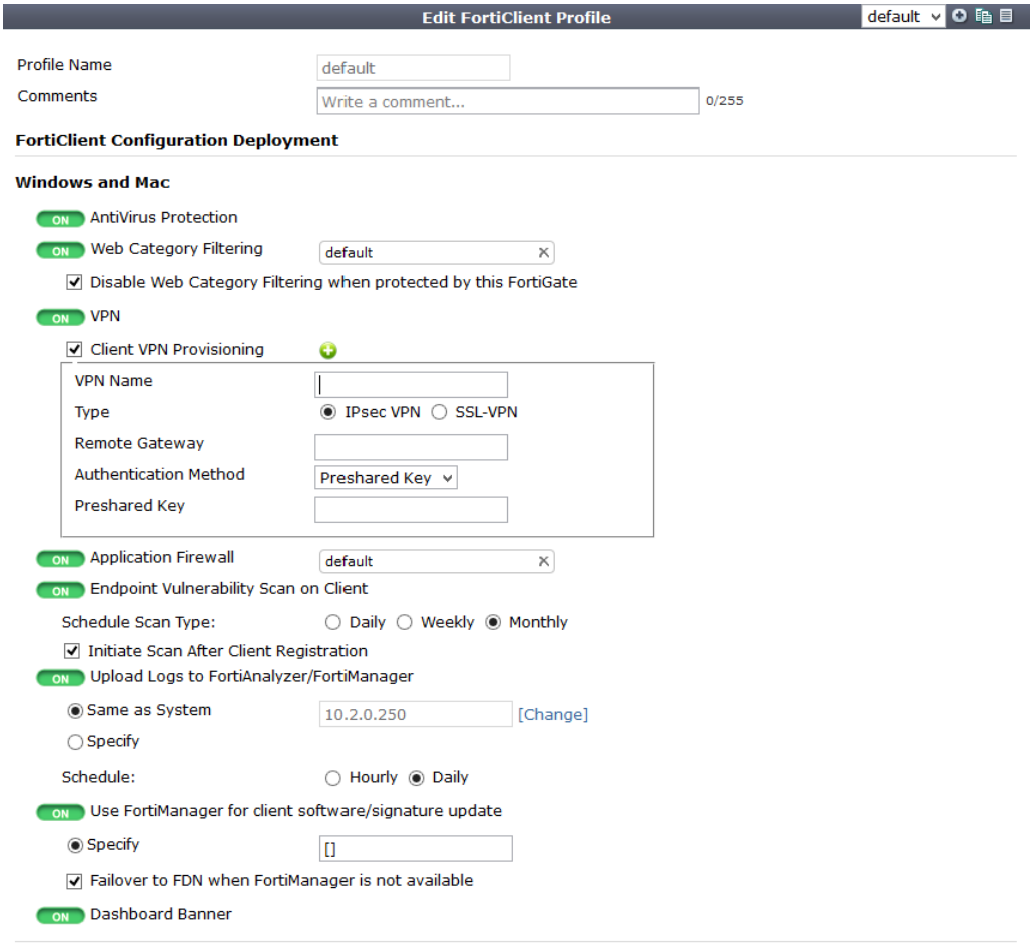
1. To configure the *FortiClient Profile*, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. You can edit the default profile for create a new FortiClient profile.

The option to assign the profile to device groups, user groups, and users is only available when selecting to create a new FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.

In FortiOS version 5.0.3 or later, you will need to enable *Multiple Security Profiles* in the *Feature Settings* to create a new FortiClient profile.

When registering to a FortiGate device, FortiClient will receive the configured FortiClient profile. The FortiClient configuration is overwritten by the FortiClient profile settings. When selecting to unregister FortiClient, the settings will reflect that of the FortiClient profile.

Figure 12: Edit FortiClient profile window



2. Configure the following settings:

Toolbar Options	Select the FortiClient profile using the drop-down menu. Select the add icon to create a new FortiClient profile. Select the clone icon to create a clone of an existing FortiClient profile. Select the view list icon to view FortiClient profiles and assignment.
Profile Name	When editing the default profile, the name cannot be changed. When creating a new FortiClient profile, XSS vulnerability characters are not allowed. Enter a name for the new FortiClient profile.
Comments	Enter a profile description. (optional)

Assign to Profile To:	Device Groups: Select device groups in the drop-down menu. Use the add icon to assign multiple device groups to the FortiClient profile, for example Mac and Windows PC. User Groups: Select user groups in the drop-down menu. Select the add icon to assign multiple user groups to the FortiClient profile. Users: Select users in the drop-down menu. Select the add icon to assign multiple users to the FortiClient profile. Note: These options are only available when creating a new FortiClient profile. Note: You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
FortiClient Configuration Deployment Windows and Mac	
AntiVirus Protection	Toggle the button on or off to enable or disable this feature.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.
VPN	Toggle the button on or off to enable or disable this feature. Select the checkbox for Client VPN Provisioning. When enabled, you can configure multiple IPsec VPN and SSL VPN connections. Select the add icon to add additional VPN connections. Enter the VPN name, type, remote gateway, and authentication method information.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down menu.
Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate.

Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select *Specify* to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address. Note: FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.
Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network when the FortiManager is not available.
Dashboard Banner	Toggle the button on or off to enable or disable this feature.

3. Select *Apply* to save the FortiClient profile setting.

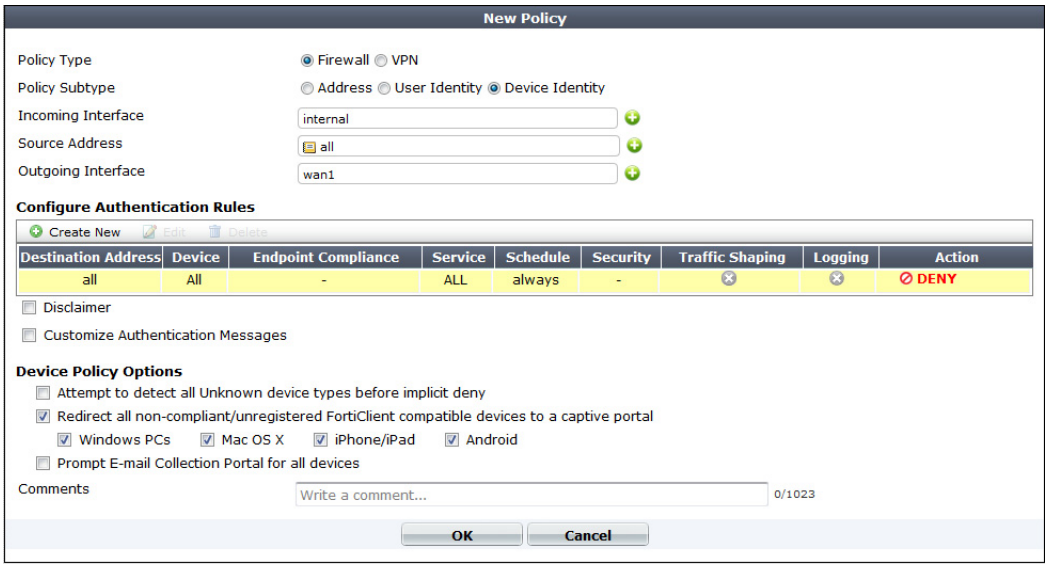
When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Configure firewall policies (Optional):

1. To configure a firewall policy for *Endpoint Management*, go to *Policy* > *Policy* > *Policy* and select *Create New* in the toolbar.

   The *New Policy* window is displayed.

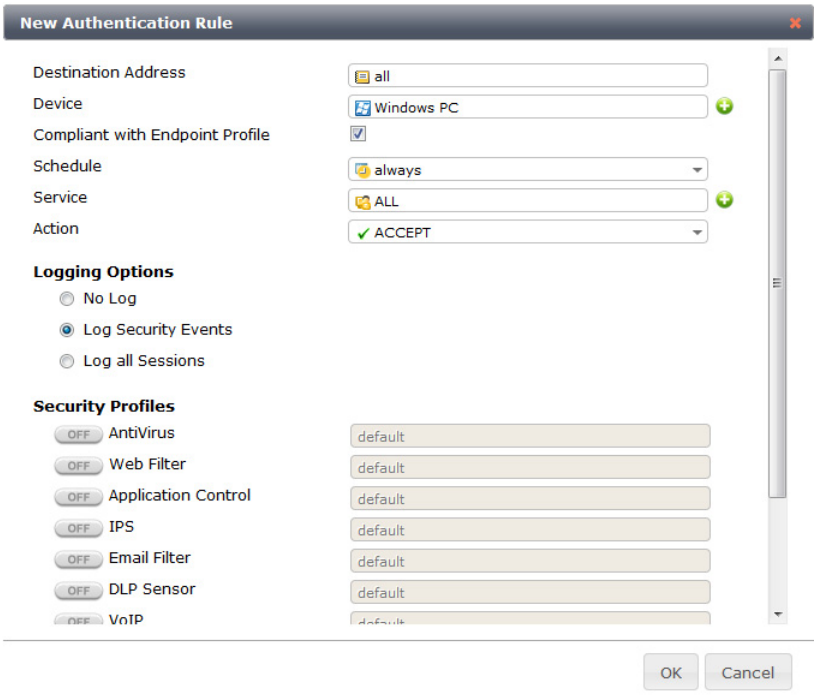
Figure 13: New policy window



2. For *Policy Type*, select *Firewall*. For *Policy Subtype*, select *Device Identity*.

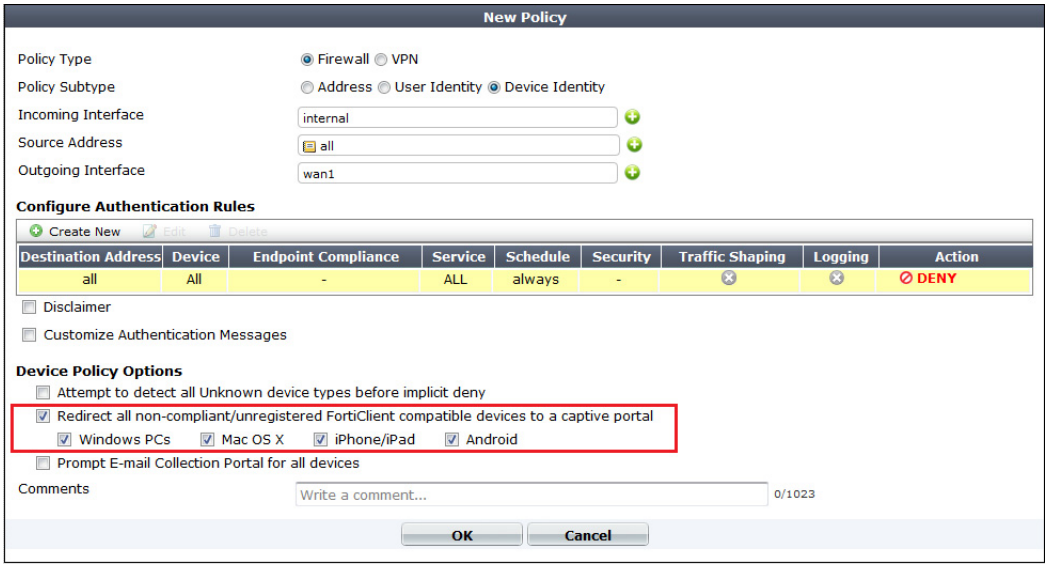
3. Configure authentication rules. Select *Create New* and add an *Accept* authentication rule for all compliant Windows-PC clients. This rule will allow Windows clients which have installed FortiClient and have been registered to this FortiGate to pass traffic.

Figure 14: Accept authentication rule for compliant Windows-PC clients.



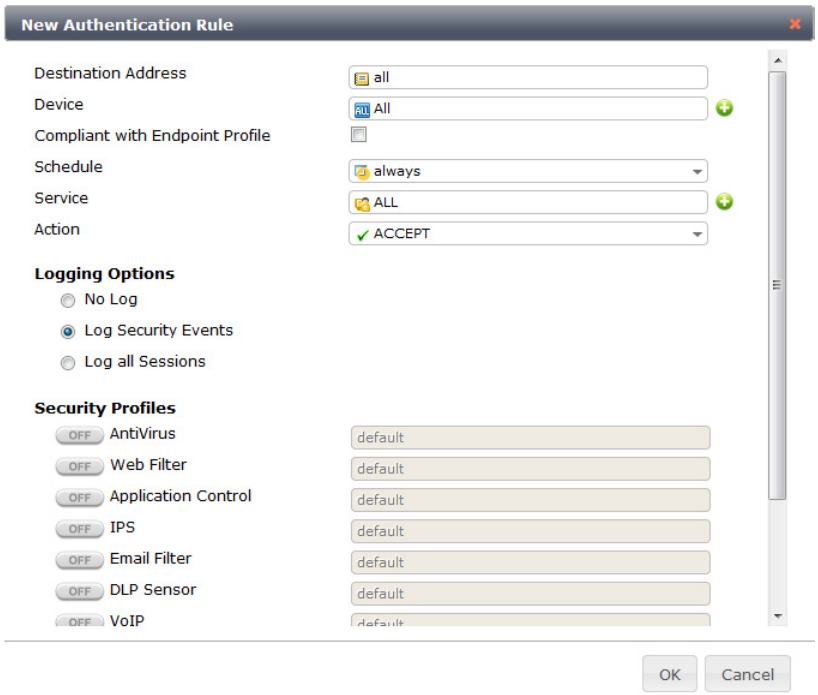
4. Select *OK* to save the rule.
5. In *Device Policy Options*, select the checkbox to *Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal*. Select the checkbox for the following: Windows PCs, Mac OS X, iPhone/iPad, and Android. Users will be redirected (via a web browser) to a dedicated portal where they can download the client. Once registered to the FortiGate, the FortiClient profile will be assigned.

Figure 15: Captive portal options



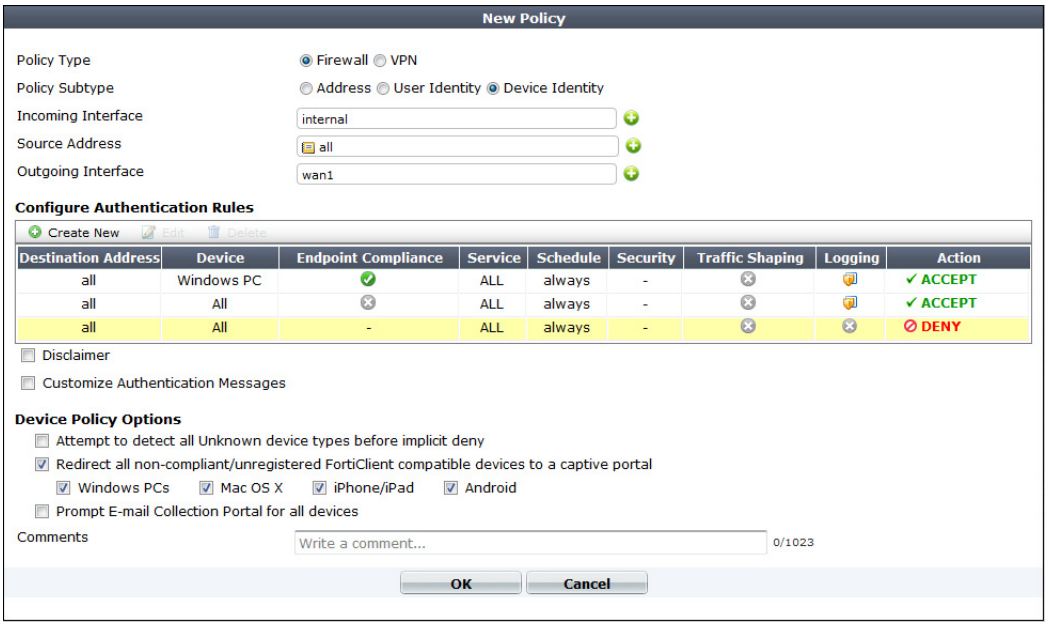
6. (Optional) Add an *Accept a*uthentication rule to allow traffic from all other devices to pass traffic without enforcing FortiClient Compliance.

Figure 16: Accept authentication rule for all other devices



Once these two authentication rules are configured, select *OK* to save the new policy setting. Your client configuration is ready for deployment.

Figure 17: New policy with authentication rules and captive portal option



After the FortiGate configuration has been completed, you can proceed with FortiClient configuration. Configure your Windows PC on the corporate network with the default gateway set to the IP of the FortiGate.

FortiClient endpoint network topologies

The following FortiClient Profile topologies are supported:

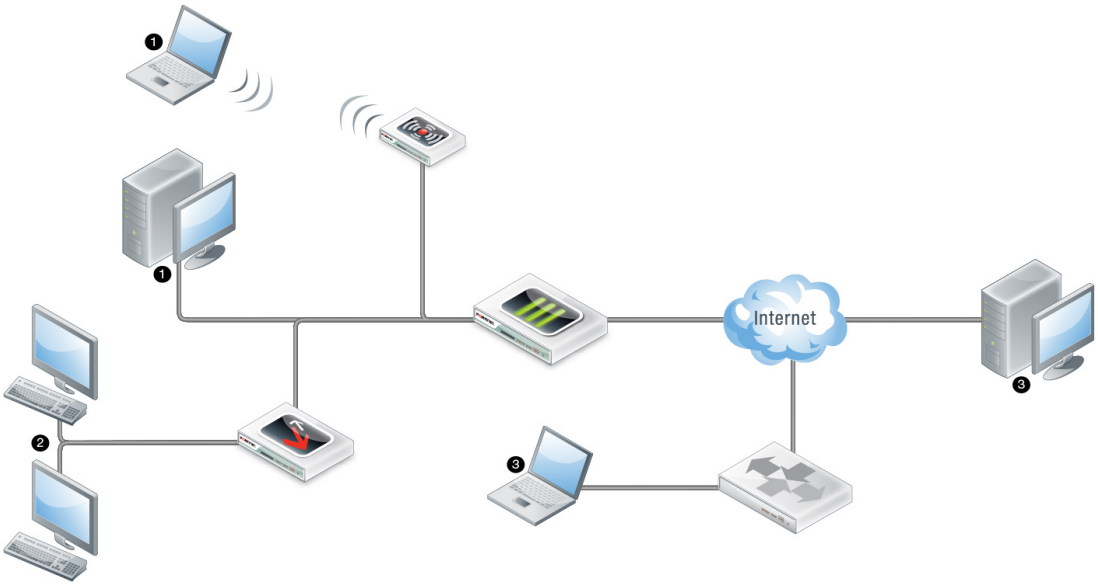
- Client is directly connected to FortiGate; either to a physical port, switch port or WiFi SSID.[1]

  This topology supports client registration, configuration sync, and FortiClient profile enforcement.
- Client is connected to FortiGate, but is behind a router or NAT device.[2]

  This topology supports client registration and configuration sync.
- Client is connected to FortiGate across a VPN connection.[3]

  This topology supports client registration, configuration sync, and FortiClient profile enforcement.

Figure 18: Network topologies



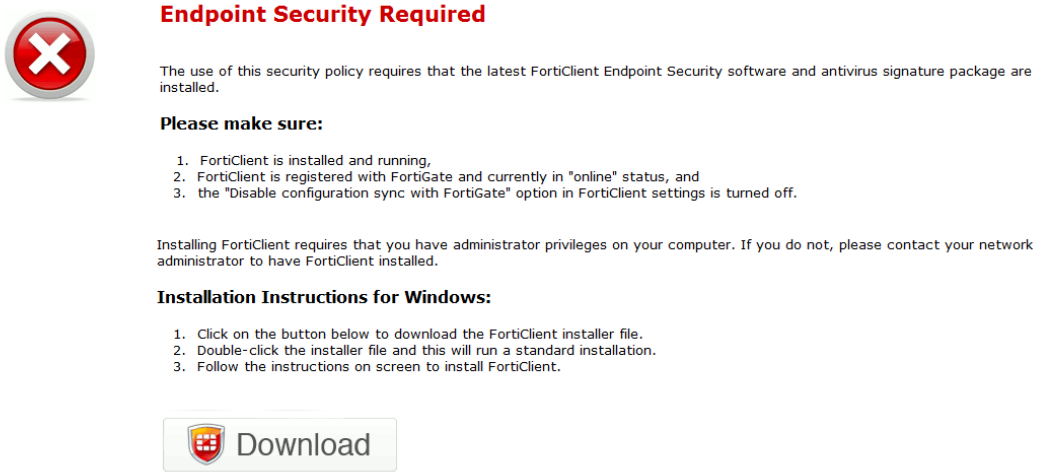
Configure FortiClient for Endpoint Management:

1. Download and install the FortiClient software.

   Open a web browser from your workstation and attempt to open a web page, the web page will be directed to the Captive Portal. Follow the instructions in the portal to download and install FortiClient.

To allow users to download FortiClient, you must enable this setting in the *SSL VPN Portal* on your FortiGate device. To enable this feature, go to *VPN* > *SSL* > *Portal* and select *Create New* in the toolbar.

Figure 19: Captive portal block page



2. Register FortiClient.

   After FortiClient completes installation, FortiClient will automatically launch and search for a FortiGate device for registration.

   There are four ways that the FortiClient/FortiGate communication is initiated:

   - FortiClient will attempt to connect to the default gateway IP address.
   - FortiClient will attempt endpoint control registration over VPN (if configured on the FortiGate)
   - FortiClient will attempt to connect to a remembered FortiGate
   - FortiClient will attempt to connect to a redundant FortiGate

Your personal computer's default gateway IP should be configured to be the IP set in the FortiGate interface.

FortiClient will search for available FortiGate devices to complete registration. You can include the option to prompt the user to enter the FortiClient registration key. Select the *Register to FortiGate* icon in the FortiClient console to retry the search.

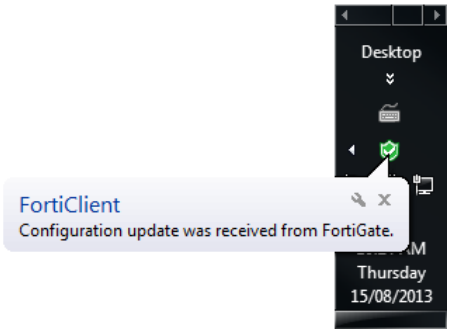
Figure 20: Registering to FortiGate dialog box

If FortiClient is unable to detect a FortiGate device, enter the IP address or URL of the device and select the *Retry* button. When FortiClient locates the FortiGate, you will be prompted to confirm the registration. Select the *Confirm* button to complete registration. Upon successful registration, the FortiGate will deploy the FortiClient profile configuration.

3. Deploy the FortiClient profile from the FortiGate device.

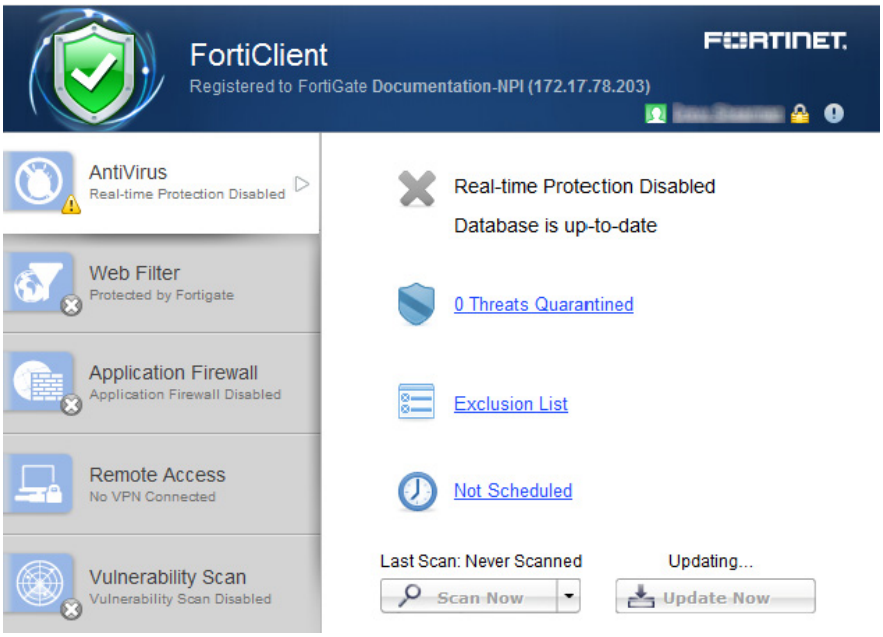
   The FortiGate will deploy the FortiClient profile after registration is complete. This FortiClient profile will permit traffic through the FortiGate. A system tray bubble message will be displayed once update is complete.

Figure 21: Configuration update notification message



The FortiClient console will display that it is successfully registered to the FortiGate. The FortiClient profile is installed on FortiClient.

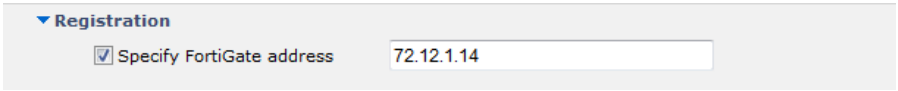
Figure 22: Registered FortiClient console



Deploy the FortiClient profile to clients over a VPN connection:

1. In the FortiClient console, select *File* > *Settings*. Under *Registration* select *Specify FortiGate address* and enter the IP address and port number (if required) of the FortiGate's internal interface.

   Figure 23: Specify FortiGate address

2. Configure an IPsec VPN connection from FortiClient to the management FortiGate.
3. Connect to the VPN.
4. You can now search for the FortiGate gateway.
5. After registration, the client is able to receive the FortiClient profile.

When creating a new FortiClient VPN (IPsec) or SSL VPN tunnel configuration on your FortiGate device, you must enable *Endpoint Registration*. See the *IPsec VPN for FortiOS 5.0* and *SSL VPN for FortiOS 5.0* sections of the *FortiOS 5.0 Handbook* for more information.

Remembered FortiGates

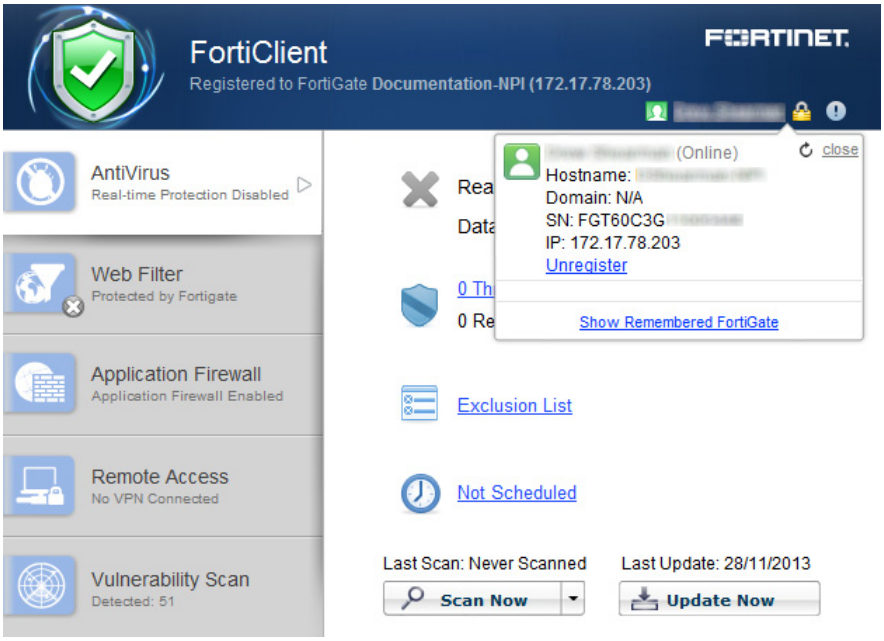
FortiClient version 5.0.1 or later adds the option to remember up to 20 FortiGate devices when accepting the broadcast registration message. FortiClient can remember and register to multiple FortiGate devices. This feature enables users to move freely between office locations and register conveniently to each FortiGate device.

When prompted to enter a registration key, FortiClient can remember the registration password.

Figure 24: Option to remember FortiGate

Select the registration icon in the console to view information for the current registered device including the hostname, domain, serial number, and IP address.

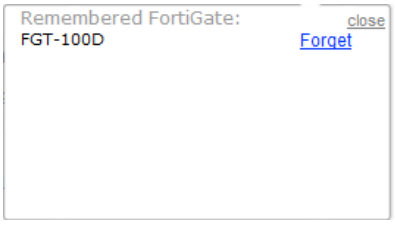
Figure 25: Remembered FortiGates



Forget a remembered FortiGate:

1. In the FortiClient console, click on the registered device name to display the registration dialog box.
2. Select *Show Remembered FortiGate* to show a list of FortiGate devices that FortiClient has previously registered with.
3. Select the device that you would like to remove from the remembered FortiGates list and select the *Forget* link.

Figure 26: Remembered FortiGates list



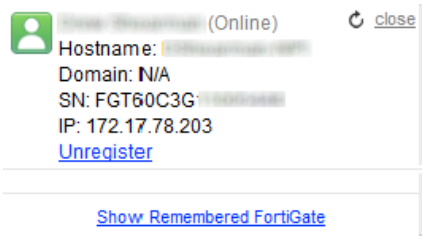
When selecting to forget a FortiGate, FortiClient will not automatically register to the FortiGate when re-connecting to the network. When the FortiGate is detected, you will be prompted to accept registration.

Unregister from FortiGate:

1. In the FortiClient console, click on the registered device name to display the registration details.

   The *Registration* dialog box appears.

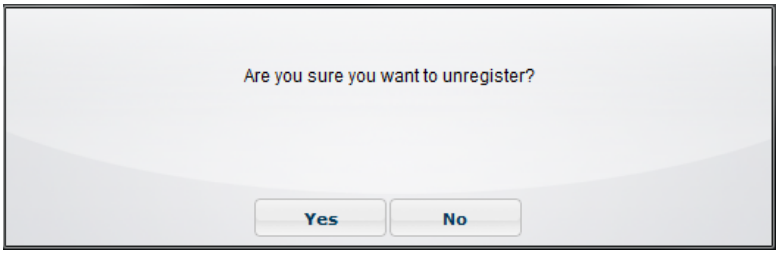
   Figure 27: Registration dialog box

2. Select *Unregister* in the registration dialog box.

   A confirmation dialog box is displayed.

   Figure 28: Confirmation dialog box

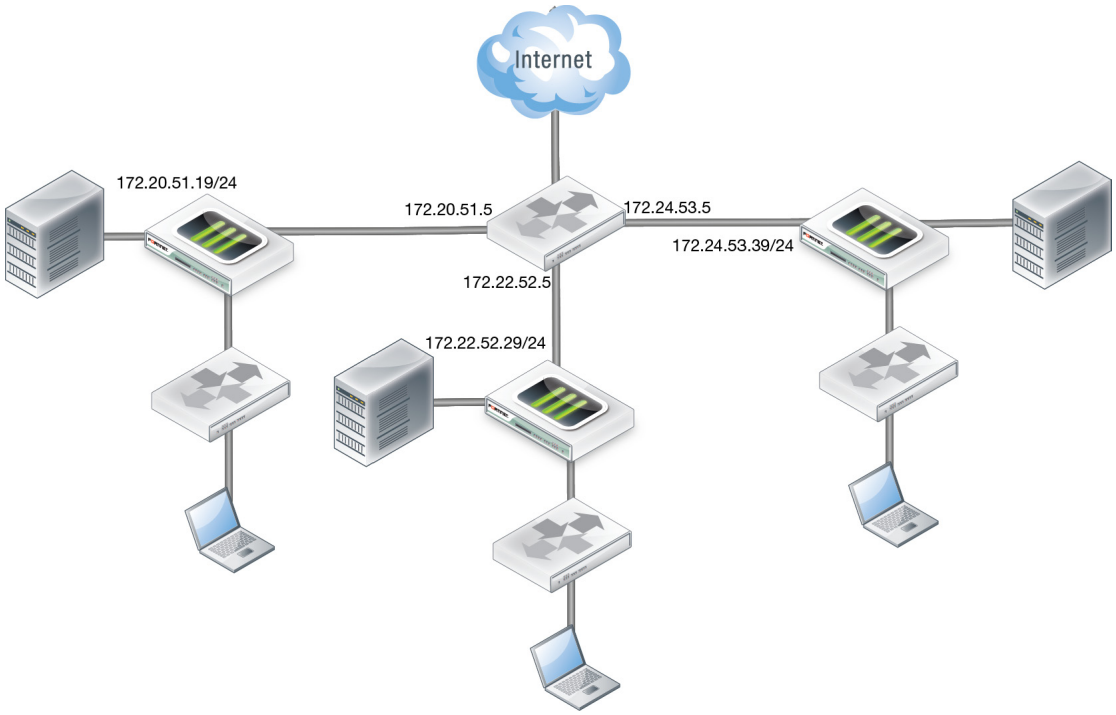
3. Select *Yes* to unregister FortiClient from the FortiGate selected.

When selecting to unregister from FortiGate, FortiClient will automatically register with the FortiGate when re-connecting to the network. To prevent this behavior, you must select to “Forget” the device.

Roaming clients (multiple redundant gateways) example

The following figure illustrates three corporate FortiGate networks. Each FortiGate can reach each other over a WAN network. FortiClient can only reach one FortiGate at a time. FortiClient may connect directly to the FortiGate or through a NAT device.

Figure 29: Roaming clients topology



If FortiClient connects through a NAT device to the FortiGate, do not enforce endpoint control compliance on the FortiGate.

On each of the three FortiGate devices configure the following:

- Interface IP addresses
- FortiClient profile
- Device identification in the interface
- FortiClient profile in the applicable firewall policy
- Endpoint control synchronization

Endpoint control synchronization allows you to synchronize endpoint control for multiple FortiGate devices. To enable endpoint control synchronization via the CLI enter the following commands on your FortiGate:

```
config endpoint-control forticlient-registration-sync
  edit 1
    set peer-ip 172.20.52.19
    next
    edit 2
    set peer-ip 172.22.53.29
  end
end
```

The IP addresses set for the peer-ip field are the WAN IP addresses for each of the FortiGate devices in the synchronization group.

You need to add the following XML configuration to FortiClient for this synchronization group. Modify the configuration file to add the following:

```
<forticlient_configuration>
  <endpoint_control>
    <!-- List of redundant FortiGates, since 5.0.2 -->
    <fortigates>
      <fortigate>
        <name>Corporate Network</name>
        <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The IP addresses are the internal IP addresses for each of the three FortiGates in the synchronization group. FortiClient can reach any of these IPs, one at a time.

If the three FortiGate devices share the same DNS name, use the following XML configuration:

```
<forticlient_configuration>
  <endpoint_control>
    <!-- List of redundant FortiGates, since 5.0.2 -->
    <fortigates>
      <fortigate>
        <name>Fortinet Americas</name>
        <addresses>fct_americas.fortinet.com</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The DNS server should return one reachable FortiGate IP address for the domain name used.

You will need to manually add FortiClient to the synchronization group when FortiClient initially registers with the FortiGate. Once added, no further action is required.

On your FortiGate, use the following CLI command to list all registered FortiClient endpoints:

```
# diagnose endpoint registration list
  FortiClient #1:
   UID                     = BA0FA25998FD4EB3A81072DC3E1799F4
   vdom                    = root
   status                  = registered
   registering time        = Tue Mar  5 15:41:36 2014
   registration expiry time = Tue Mar 12 15:41:36 2014
   source IP               = 192.168.10.100
   user                    = lindseyk
   host OS                = Microsoft Windows 7 Enterprise Edition,
       64-bit Service Pack 1 (build 7601)
   local registration      = no
   remote registration SN  = FG10DH3G11604696
```

The `local registration` entry indicates whether this specific FortiClient is registered to this FortiGate, or to another FortiGate within the synchronization group.

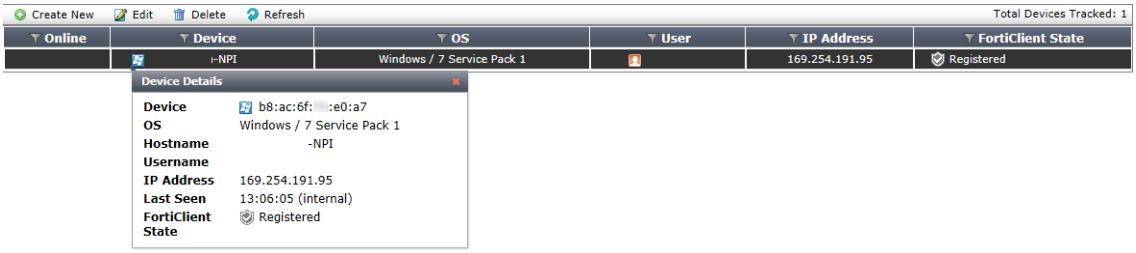
If any of the FortiGate devices require a password to complete registration, you can use the following XML configuration to provide password information to FortiClient:

```
<forticlient_configuration>
  <endpoint_control>
    <!-- List of redundant FortiGates, since 5.0.2 -->
    <fortigates>
      <fortigate>
        <name>Corporate Network</name>
        <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
        <registration_password>uNbre@kab1e</registration_password>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

View FortiClient registration in the FortiGate Web-based Manager

You can view all registered FortiClient agents in the FortiGate Web-based Manager. Each new registration will be automatically added to the device table. To view registered devices go to *User & Devices* > *Device* > *Device Definition*. The state for the new FortiClient registration is listed as *Registered*.

Figure 30: FortiGate device details

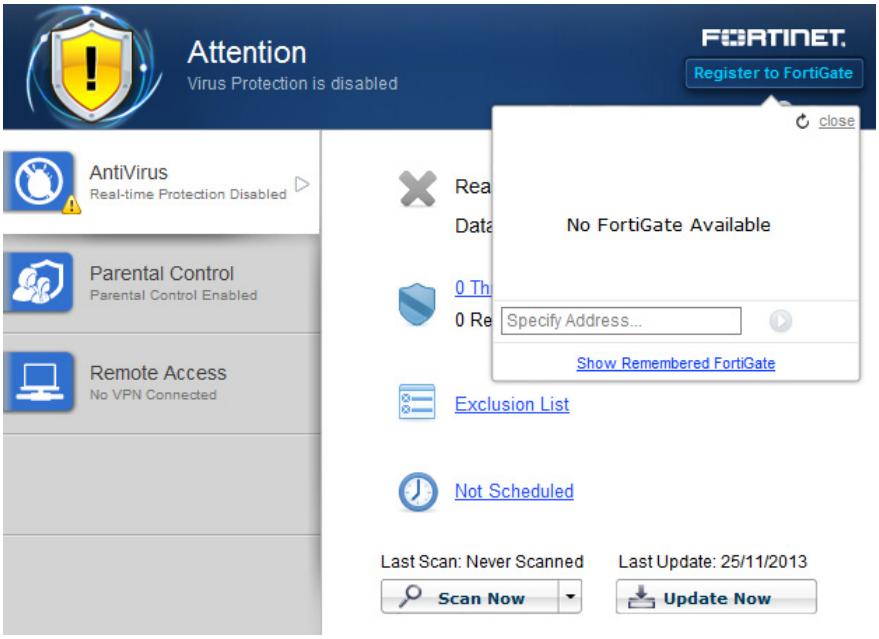


Configure the FortiGate IP in FortiClient for registration

The FortiClient administrative user can specify a FortiGate IP address for registration and client configuration management. When an unregistered FortiClient starts up, FortiClient will list all reachable FortiGates for endpoint control registration in the registration drop-down list. The list will include any FortiGate that sends endpoint control broadcasts. Select the FortiGate icon in the FortiClient console to list discovered FortiGates. Any IP address provided in the *Settings* page under the *Registration* element is included in the list.

To configure a FortiGate IP address in FortiClient, select the *Register to FortiGate* button in the FortiClient console. In the *Specify Address* field, enter the IP address and port number (if required) of the FortiGate's internal interface.

Figure 31: Configure FortiGate in FortiClient

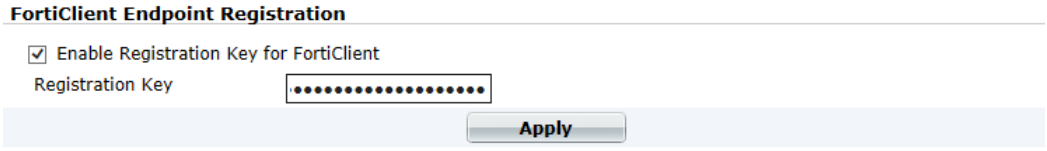


The FortiClient settings are locked, and cannot be modified after registration to a FortiGate is completed.

Enable FortiClient endpoint registration key (optional)

To enable *FortiClient Endpoint Registration Key* in the FortiGate Web-based Manager, select *System* > *Config* > *Advanced*. Select *Enable Registration Key for FortiClient*, enter the *Registration Key* and select *Apply*.

Figure 32: Enable FortiClient endpoint registration key on FortiGate



The FortiClient user will need to enter the same registration key to successfully register FortiClient to the FortiGate.

Update FortiClient registration license on FortiGate

To update the FortiClient registration license on FortiGate, use the following CLI command:

```
execute FortiClient-NAC update-registration-license <license
    key/activation code>
```

Endpoint registration with Active Directory (AD) user groups

The user's AD domain name and group are both sent to the FortiGate during endpoint registration. Administrators may configure the FortiGate to deploy endpoint and/or firewall profiles based on the end user's AD domain group. This feature requires FortiClient version 5.0.4 or later and FortiOS version 5.0.3 or later.

The following steps are discussed in more details:

- Configure users and groups on your AD server
- Configure your FortiAuthenticator
- Configure your FortiGate
- Connect to the FortiGate using FortiClient endpoint
- Monitoring client registrations

Configure users and groups on your AD server

Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time. Groups may be nested.

Configure your FortiAuthenticator

Configure FortiAuthenticator to use the AD server that you created. For more information see the *FortiAuthenticator Administration Guide*.

Configure your FortiGate

Configure FortiGate from the Web-based Manager as listed below.

Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO):

1. Go to *User & Device* > *Authentication* > *Single Sign-On*.
2. Select *Create New* in the toolbar.

   The *New Single Sign-On Server* window opens.

   Figure 33: New single sign-on server window

3. In the type field, select *Fortinet Single-Sign-On Agent*.

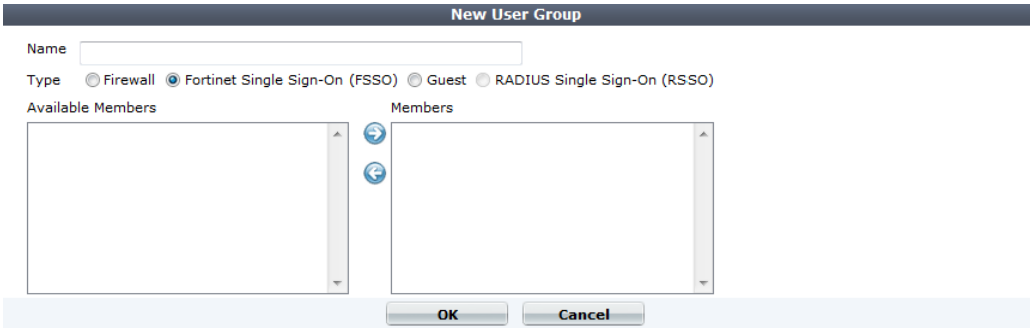
4. Enter the information required for the agent. This includes the name, primary and secondary IP address and password. Select an LDAP server in the drop-down menu if applicable. Select *More FSSO agents* to add up to three additional agents.
5. Select *OK* to save the agent configuration.

Create a user group:

1. Go to *User & Device* > *User* > *User Groups*.
2. Select *Create New* in the toolbar.

   The *New User Group* window opens.

Figure 34: New user group window



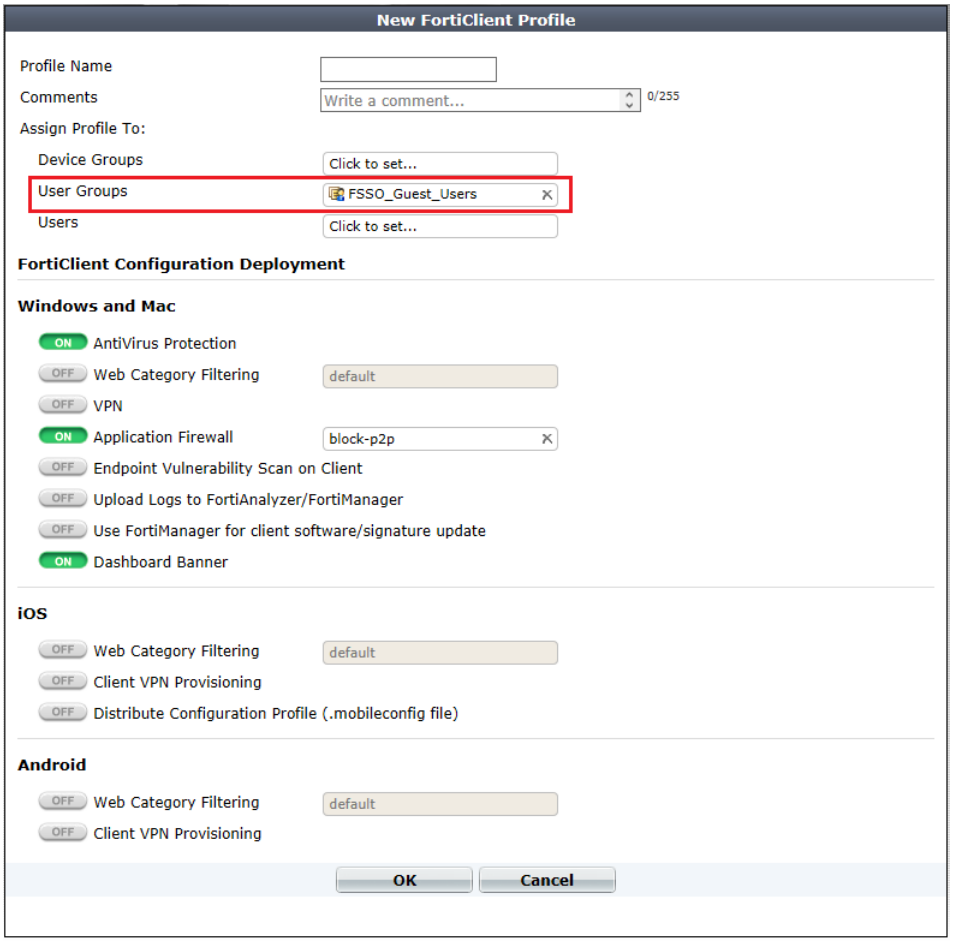
3. In the type field, select *Fortinet Single-Sign-On (FSSO)*.
4. Enter a name for the new group and select members from the available members using the right and left directional arrow icons.
5. Select OK to save the group configuration.

Configure the FortiClient profile:

1. Go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
2. In the toolbar, select the add icon to create a new FortiClient profile.

   The *New FortiClient Profile* window opens.

Figure 35: New FortiClient Profile



3. Enter a profile name and optional comments.
4. In the *User Groups* drop-down menu select the FSSO user group(s).
5. Configure FortiClient configuration deployment as required.
6. Select *OK* to save the new FortiClient profile.

Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who register successfully but have no matching FortiClient profile.

Configure the firewall policy:

Configure the firewall policy as described in "Configure endpoint management" on page 34. Ensure that *Compliant with FortiClient Profile* is selected in the *Authentication Rules* dialog box.

Connect to the FortiGate using FortiClient endpoint

The Microsoft Windows system on which FortiClient is installed should join the domain of the AD server configured earlier. Users may login with their domain user name.

Following this, FortiClient endpoint registrations will send the logged-in user's name and domain to the FortiGate. The FortiGate will assign the appropriate profiles based on the configurations.

Monitoring client registrations

The following FortiOS CLI command lists information about registered clients. This includes domain-related details for the client (if any).

```
diagnose endpoint record-list
Record 1:
  IP_Address = 172.172.172.111(1)
  MAC_Address = 00:0C:00:00:1A:54
  Host MAC_Address = 00:0C:00:00:1A:54
  VDOM = root
  Registration status: Forticlient installed but not registered
  Online status: offline
  FCC connection handle: 2
  FortiClient version: 5.0.9
  AVDB version: 21.997
  FortiClient app signature version: 4.412
  FortiClient vulnerability scan engine version: 1.339
  FortiClient feature version status: 0
  FortiClient UID: 07A1F8489C9F4A21BE910481ACA0442D (0)
  FortiClient config dirty: 0:1:1
  FortiClient server config: 7cb6a441eb85873f9cf4bb8c11adade4::
  FortiClient config: 0
  FortiClient iOS server mconf:
  FortiClient iOS mconf:
  FortiClient iOS server ipsec_vpn mconf:
  FortiClient iOS ipsec_vpn mconf:
  Endpoint Profile: engineering_team
  Auth_AD_groups:
  Auth_group: engineering
  Auth_user: thomasp
  Host_Name: Eng_Client72
  OS_Version: Microsoft Windows 7 Enterprise Edition, 64-bit Service
      Pack 1 (build 7601)
  Host_Description: AT/AT COMPATIBLE
  Domain:
  Last_Login_User: thomasp
  Host_Model: OptiPlex 390
  Host_Manufacturer: Dell Inc.
  CPU_Model: Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz
  Memory_Size: 4096
  Installed features: 55
  Enabled features: 52
  System Uptime: 3012
  FortiClient log upload: 0 since Wed Dec 31 17:00:00 2014
  Last connection: Mon Mar 25 08:52:56 2014
```

Antivirus

FortiClient Antivirus

FortiClient version 5.0 includes an antivirus module to scan system files, executable files, dynamic-link library (DLL) files, and drivers. FortiClient will also scan for and remove rootkits.

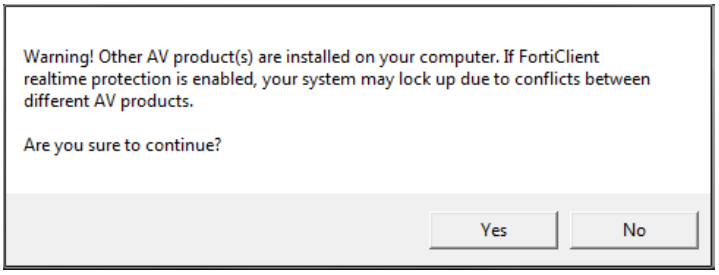
This section describes how to enable antivirus and configuration options.

Enable/disable antivirus

To enable or disable FortiClient antivirus real-time protection, toggle the *[Enable/Disable]* option in the FortiClient console.

If you have another antivirus program installed on your system, FortiClient will prompt the following dialog box warning that your system may lock up due to conflicts between different AV products.

Figure 36: Conflicting antivirus warning

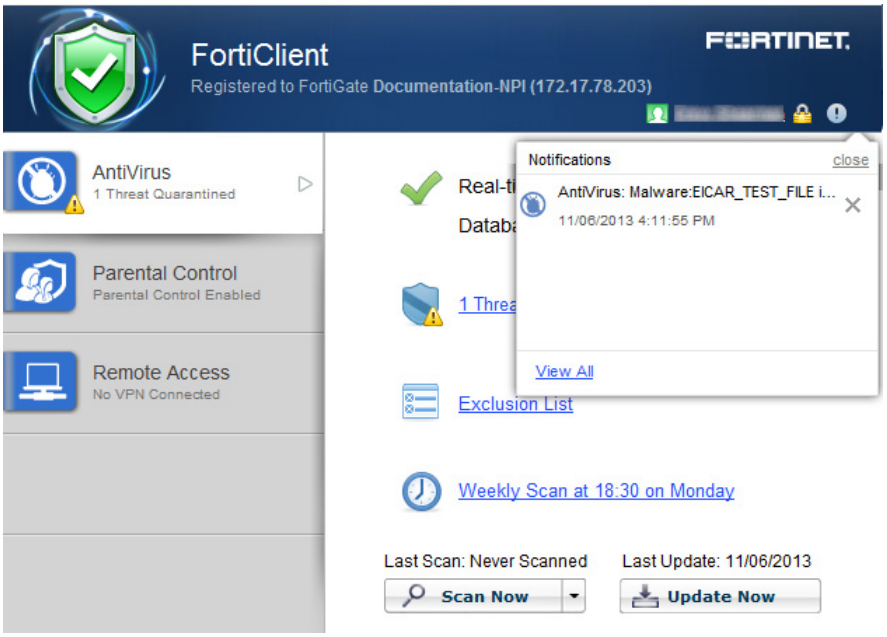


It is recommended to remove the conflicting antivirus product before installing FortiClient or enabling the antivirus real-time protection feature.

Notifications

Select the notifications icon in the FortiClient console to view all notifications. When a virus has been detected, the notifications icon will change from gray to yellow. Select *View All* to view all antivirus event notifications.

Figure 37: Antivirus notifications dialog box



Scan now

To perform on-demand antivirus scanning, select the *Scan Now* button in the FortiClient console. Use the drop-menu to select *Custom Scan, Full Scan*, or *Quick Scan*. The console displays the date of the last scan above the button.

Custom Scan runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.

Full Scan runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executable files, DLLs, and drivers for threats.

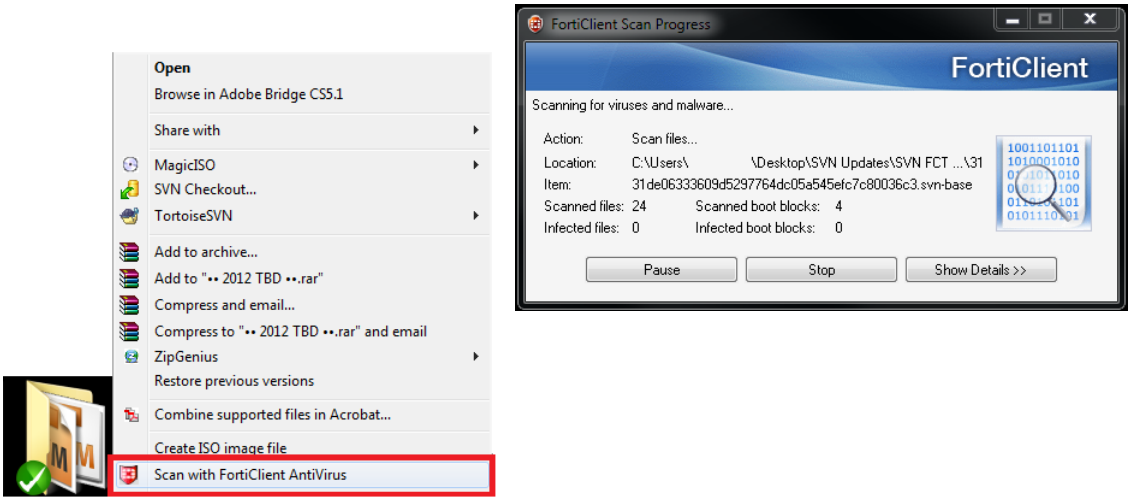
Quick System Scan runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, DLLs, drivers that are currently running for threats.

Figure 38: Antivirus scan options

Scan a file or folder on your workstation

To perform a virus scan a specific file or folder on your workstation, right-click the file or folder and select *Scan with FortiClient AntiVirus*.

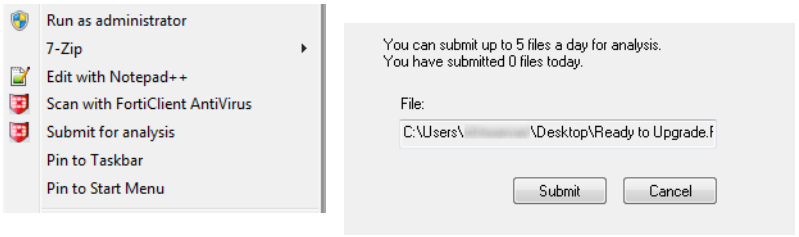
Figure 39: Scan a specific file or folder



Submit a file for analysis

You can select to send up to 5 files a day to FortiGuard for analysis. To submit a file, right-click a file or executable and select Submit for analysis from the menu. A dialog box will be displayed which allows you to see the number of files you have submitted. Confirm the file location of the file you want to submit and select the *Submit* button.

Figure 40: Submit files for analysis



You do not receive feedback for files submitted for analysis. The FortiGuard team uses this feedback to create signatures for any files which are submitted for analysis and determined to be malicious.

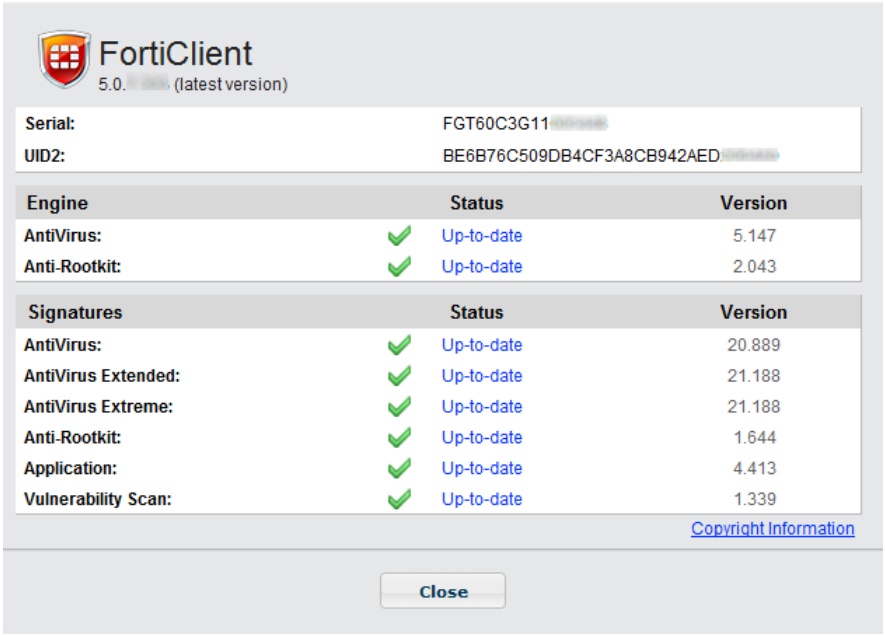
Update now

To perform on-demand update of FortiClient version, engines, and signatures, select the *Update Now* button in the FortiClient console. The console notes the date of the last update above the button.

To view the current FortiClient version, engine, and signature information, select *Help* in the toolbar, and select *About* in the drop-down menu.

You can select to use a FortiManager device for client software and signature updates. When configuring the FortiClient profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

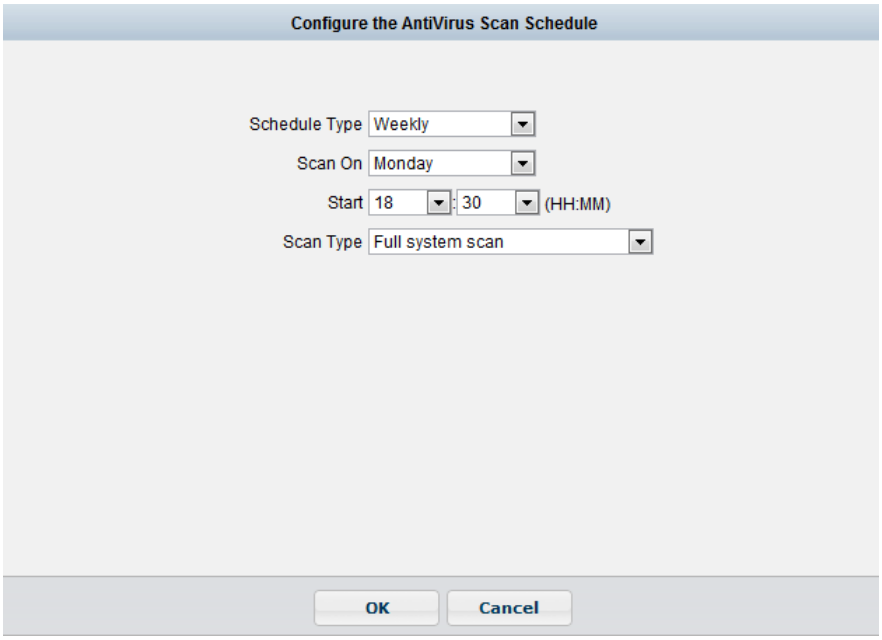
Figure 41: About FortiClient page



Schedule antivirus scanning

To schedule antivirus scanning, select *Weekly Scan* in the content pane.

Figure 42: Antivirus scheduling page



Configure the following settings:

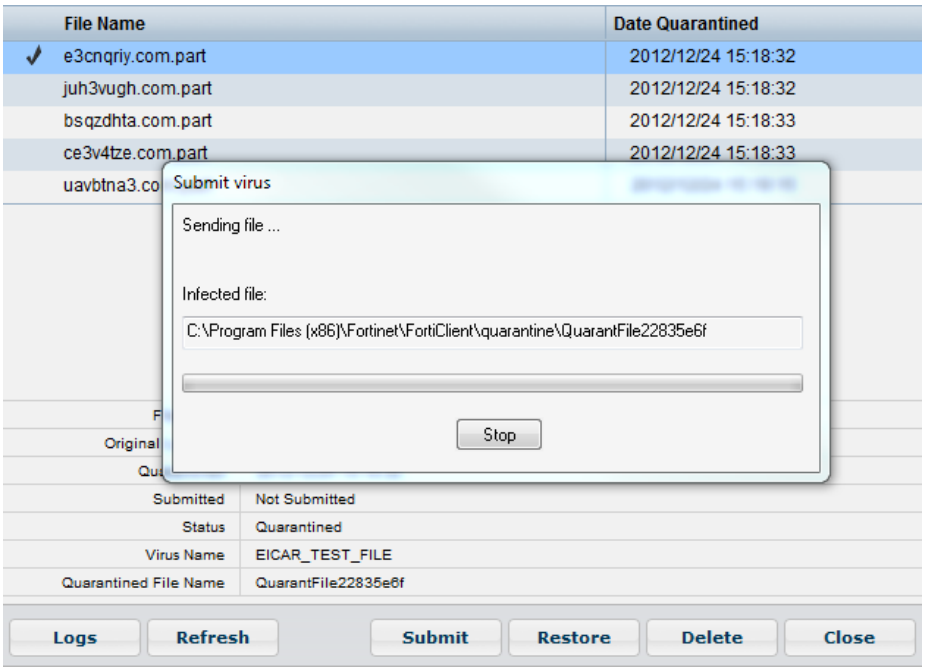
Schedule Type	Select Daily, Weekly or Monthly in the drop-down menu.
Scan On	For Weekly scheduled scan, select the day of the week in the drop-down menu. For Monthly scheduled scan, the day of the month in the drop-down menu.
Start	Select the start time in the drop-down menus. The time format is represented in hours and minutes, 24-hour clock.
Scan Type	Select the scan type: Custom Scan runs the rootkit detection engine to detect and remove rootkits. Custom Scan allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. Full Scan runs the rootkit detection engine to detect and remove rootkits. Full Scan then performs a full system scan including all files, executable files, DLLs, and drivers for threats. Quick System Scan runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, DLLs, drivers that are currently running for threats.

Select *OK* to save the setting.

View quarantined threats

To view quarantined threats, select *Threats Quarantined* in the FortiClient console. In this page you can view, restore, or delete the quarantined file. You can also submit the file to FortiGuard.

Figure 43: Threats quarantined page



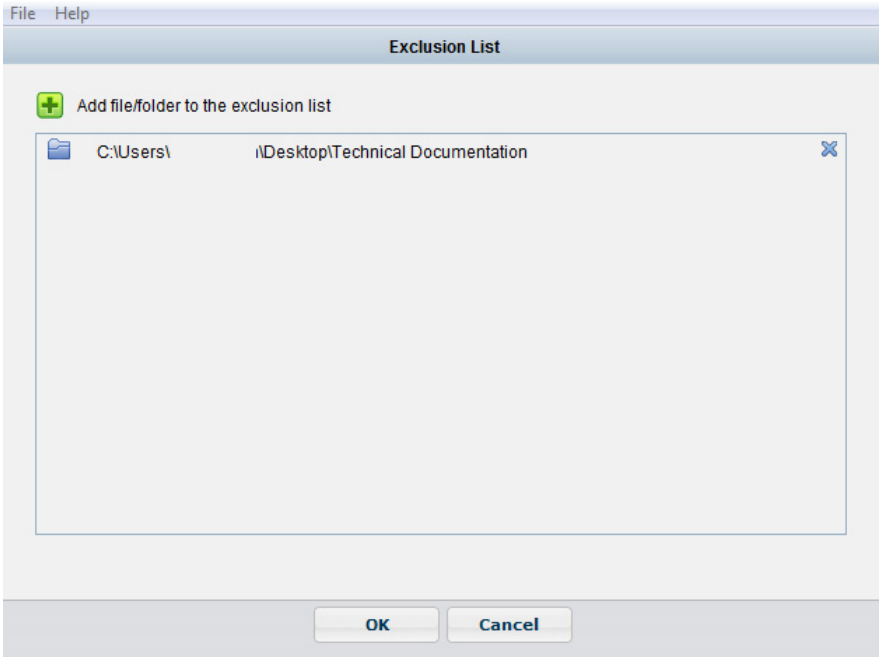
This page displays the following:

File Name	The name of the file.
Date Quarantined	The date and time that the file was quarantined by FortiClient.
File Information	Select a file from the list to view detailed information including the quarantined location, status, virus name, and quarantined file name.
Logs	Select to view FortiClient log data.
Refresh	Select to refresh the list.
Submit	Select to submit the quarantined file to FortiGuard.
Restore	Select to add the selected file/folder to the exclusion list.
Delete	Select to delete the quarantined file.
Close	Select to close the page and return to the FortiClient console.

Add files/folders to an exclusion list

To add files/folders to the antivirus exclusion list, select *Exclusion List* in the content pane. In the following configuration page, select the plus '+' symbol to add files or folders to the list. Any files or folders in this exclusion list will not be scanned.

Figure 44: Antivirus exclusion list page

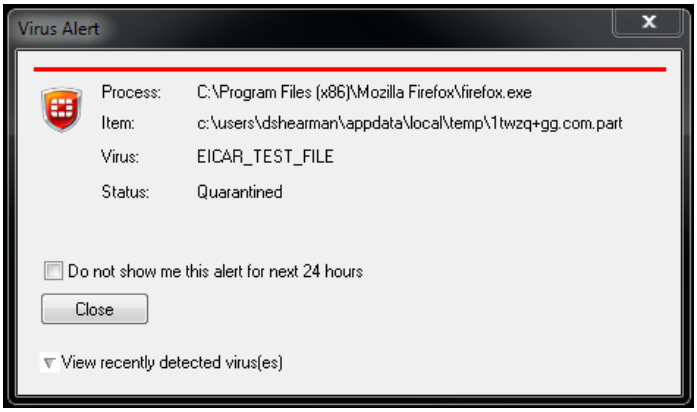


Select *OK* to save the setting.

Antivirus warning

When FortiClient antivirus detects a virus while attempting to download a file via a web-browser, you will receive a warning dialog message similar to Figure 45. Browse to the *Threat Quarantine* menu in the console to view details for the detected threat.

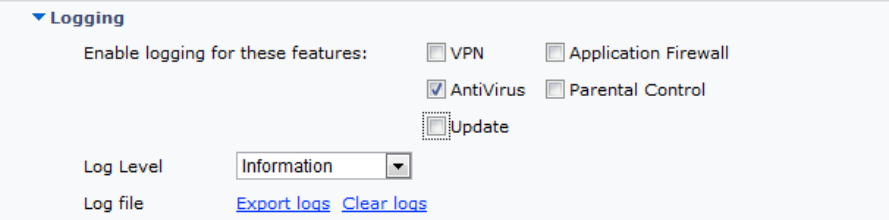
Figure 45: Example virus warning message



Antivirus logging

To configure antivirus logging, select *File* in the toolbar and *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu.

Figure 46: Logging options



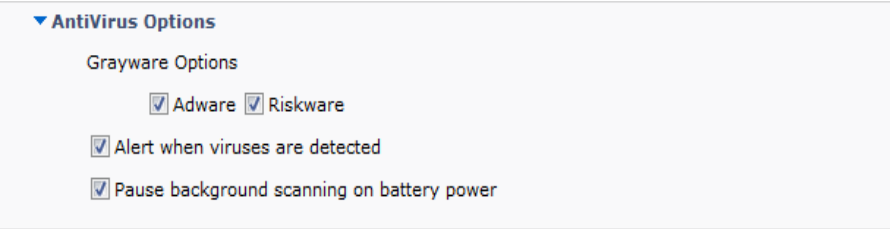
Configure the following settings:

Logging	
Enable logging for these features	Select antivirus to enable logging for this feature.
Log Level	Select the level of logging: • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and functionality could be affected. • Warning: Functionality could be affected. • Notice: Information about normal events. • Information: General information about system operations. • Debug: Debug FortiClient.
Log file	
Export logs	Select to export logs to your local hard disk drive (HDD) in .log format.
Clear logs	Select to clear all logs. You will be presented a confirmation window, select *Yes* to proceed.

Antivirus options

To configure antivirus options, select *File* in the toolbar, and *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure options outlined in the following figure and table.

Figure 47: Antivirus options



Configure the following settings:

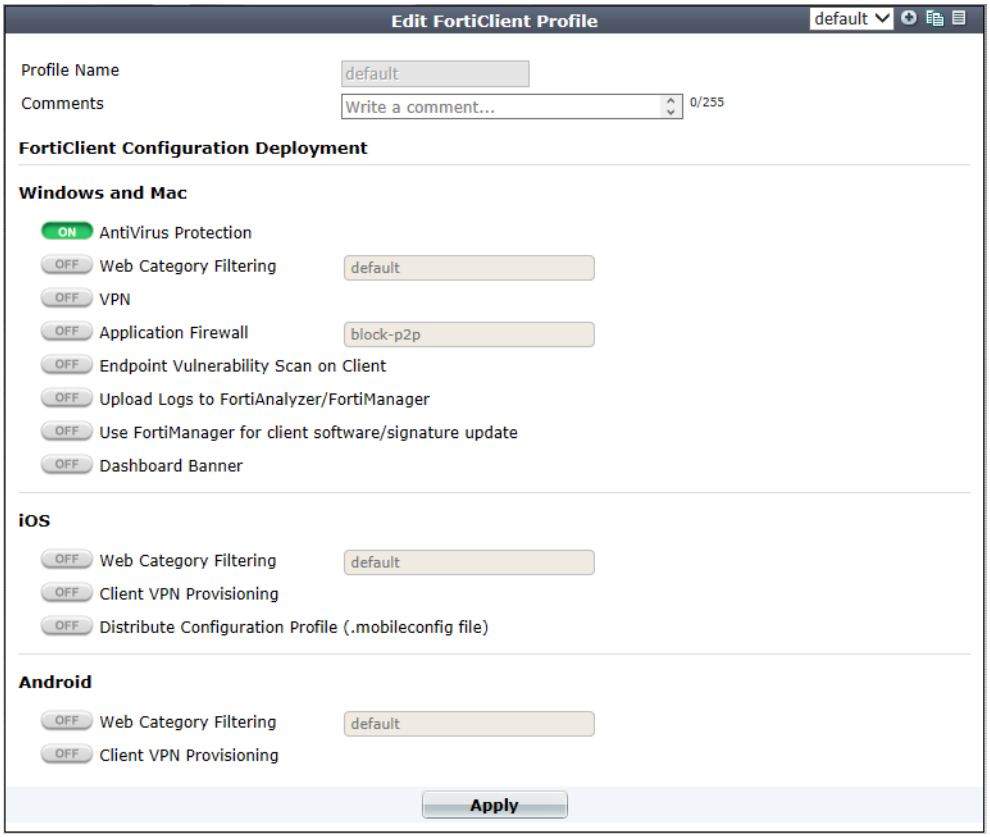
Antivirus Options	
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer.
Pause background scanning on battery power	Select to pause background scanning when your personal computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

When registered to FortiGate, you can select to enable or disable FortiClient Antivirus Protection in the FortiClient Profile.

To enable Antivirus Realtime Protection in the FortiClient Profile:

1. Login to your FortiGate.
2. In the left tree menu, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
3. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *AntiVirus Protection* button to *ON*.

Figure 48: Edit FortiClient Profile



4. Select *Apply* to save the profile.
   The FortiGate will send the FortiClient Profile configuration update to registered clients.

Figure 49: Configuration update was received from FortiGate.

Parental Control/Web Filtering

Parental Control/Web Filtering allows you to block, allow, warn, and monitor web traffic based on URL category. URL categorization is handled by the FortiGuard Distribution Network (FDN).

When FortiClient is registered to a FortiGate, the *Parental Control* module will reflect *Web Filtering*. You can disable *Web Category Filtering* in FortiClient from the FortiGate FortiClient profile. If the FortiClient device is behind a FortiGate, the client device will use the web filter profile from the FortiGate.

The FortiClient Endpoint Control feature enables the site administrator to distribute Web Filtering profile from a FortiGate device. The overall process is as follows:

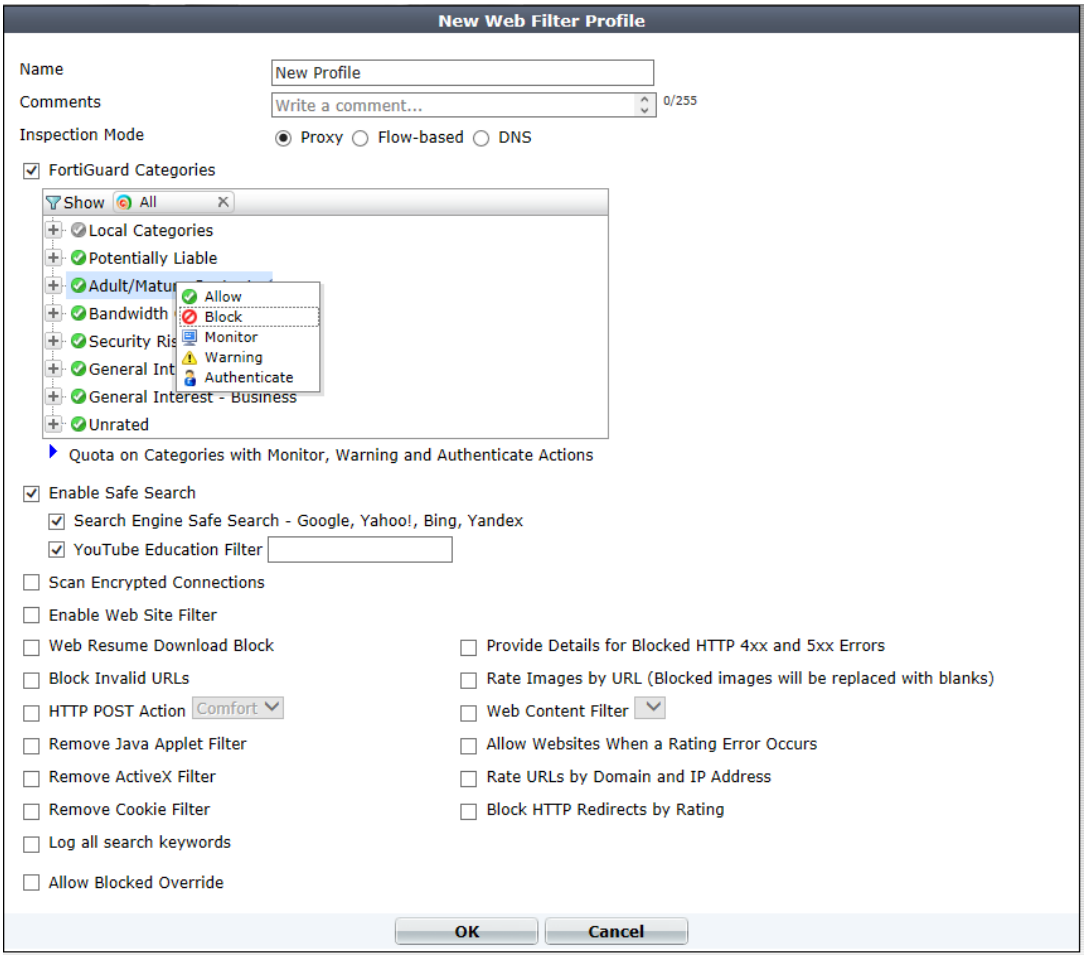
- Create a Web Filter profile on the FortiGate
- Add the Web Filter profile to the FortiClient Profile on the FortiGate

Step 1: Create a Web Filter Profile

Use the following steps to create a custom Web Filter profile in the FortiGate Web-based Manager:

1. Login to the FortiGate
2. In the left tree menu, select *Security Profiles* > *Web Filter* > *Profiles*.
3. To create a new profile, click the add icon in the upper-right corner. The *New Web Filter Profile* page opens.

Figure 50: New web filter profile page



4. Enter a name for the profile.
5. Select the *FortiGuard Categories* checkbox. This will allow you to modify the categories.

If the FortiGate device is not licensed, you will receive an dialog box advising that traffic may be blocked if this option is enabled.

FortiClient supports the following Web Filter Profile settings: FortiGuard Categories and Enable Safe Search. All other settings apply to FortiGate only.

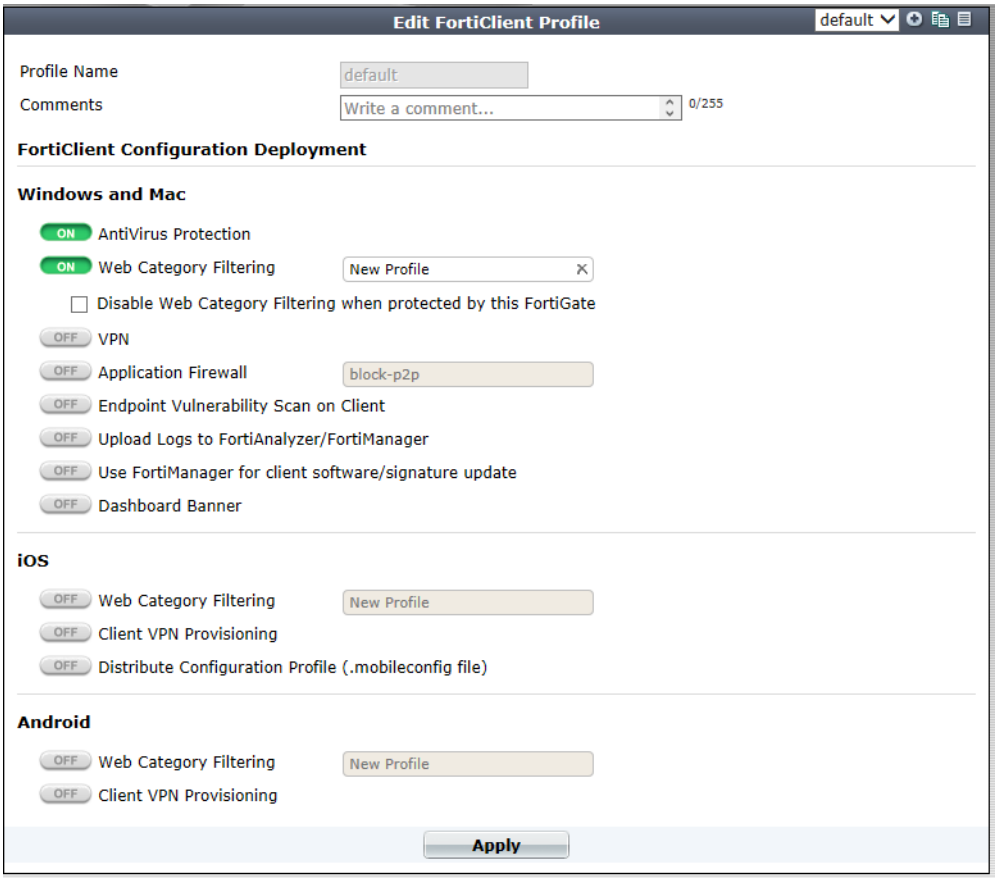
6. Modify a category. For example, right-click on the *General Interest – Business* category. In the menu, select the *Block* option.
7. Block a sub-category. For example, click the *General Interest – Personal* group to expand the category menu. Scroll down to where the *Games* sub-category is located. Right-click the *Games* sub-category, and select the *Block* option.
8. Select to enable safe search. You can select the checkbox to enable search engine safe search and YouTube education filter.

9. Select *Apply* to save the profile.

Step 2: Add the Web Filter profile to the FortiClient Profile

1. In the left tree menu, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
2. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *Web Category Filtering* button to *ON*.

Figure 51: Edit FortiClient Profile



3. Select the Web Filter profile in the drop-down list.
4. Uncheck the checkbox for *Disable Web Category Filtering when protected by this FortiGate*.
5. Click *Apply* to save the profile.

   The FortiGate will send the FortiClient Profile configuration update to registered clients.

Figure 52: Configuration update was received from FortiGate

The Web Filtering module is now available in FortiClient.

Figure 53 illustrates web filter profile settings received by the FortiGate endpoint control profile.

Figure 53: Web filter settings in the FortiClient profile

When FortiClient is not registered to FortiGate, you can enable or disable the Parental Control feature. You can define what sites are allowed or blocked and view violations.

Enable/Disable Parental Control

To enable or disable FortiClient Parental Control/Web Filtering, toggle the *[Enable/Disable]* button in the FortiClient console. Parental Control is enabled by default.

Figure 54: Parental control module

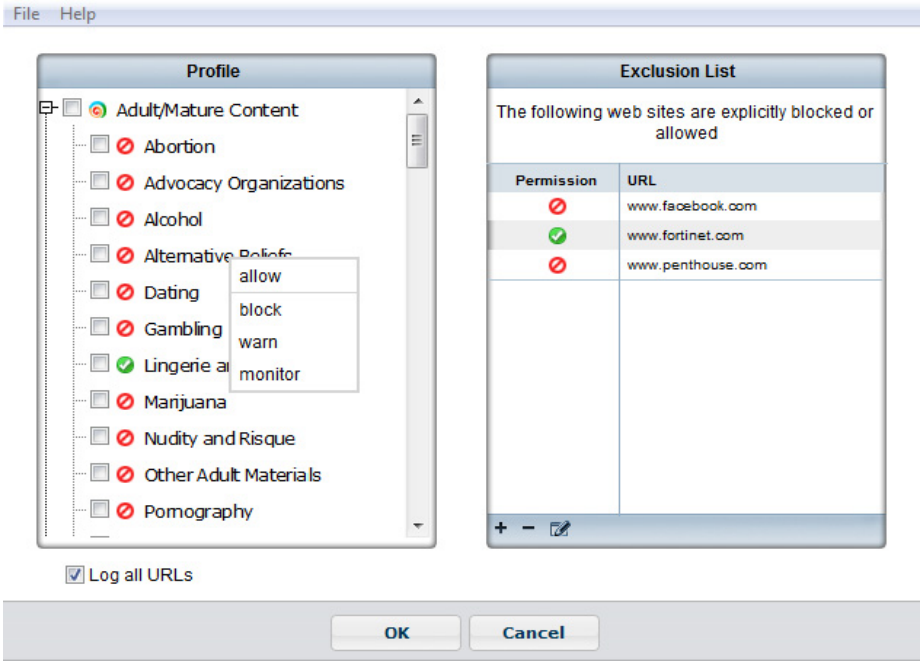
Enable/Disable	Toggle to enable or disable Parental Control.
Settings	Select to configure the Parental Control profile.

Parental Control settings

You can configure a profile to allow, block, warn, or monitor web traffic based on category under *Profile*. Use the right-click menu to set the action for the full category or sub-category.

You can add websites to the exclusion list and set the permission to allow or block. If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.

Figure 55: Profile and exclusion list



Configure the following settings:

Profile	Select to allow, block, warn or monitor traffic by category or sub-category.
Exclusion List	Select to exclude websites that are explicitly blocked or allowed. Use the add icon to add websites and the minus (-) icon to delete websites from the list.
Log all URLs	Select to log all URLs.
Enable Safe Search	Select to enable safe search.
Search Engine Safe Search	Select to enable search engine safe search for Google, Yahoo!, Bing, and Yandex.
YouTube Education Filter	Select to enable the YouTube educational filter and enter your filter code. The filter blocks non-educational content as per your YouTube filter code.

See http://support.google.com/youtube/bin/answer.py?hl=en&answer=2592715 for more information on YouTube for schools and the education filter.

View profile violations

To view profile violations, select *Violations (in the Last 7 Days)* in the FortiClient console.

Figure 56: Traffic violations

Website	Category	Time	User
ffupdate.conduit-services.com	Malicious Websites	25/10/2012 9:53:37 AM	dshearman

Application Firewall

FortiClient version 5.0 can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application.

In FortiClient version 5.0.4 or later this feature is disabled by default and the tab is hidden for standalone clients. For uses who are registered to a FortiGate using endpoint control, the FortiGate administer may choose to enable this feature.

In FortiClient version 5.0.4 or later, the application firewall feature is enabled in the FortiClient Profile. The profile includes application firewall configuration.

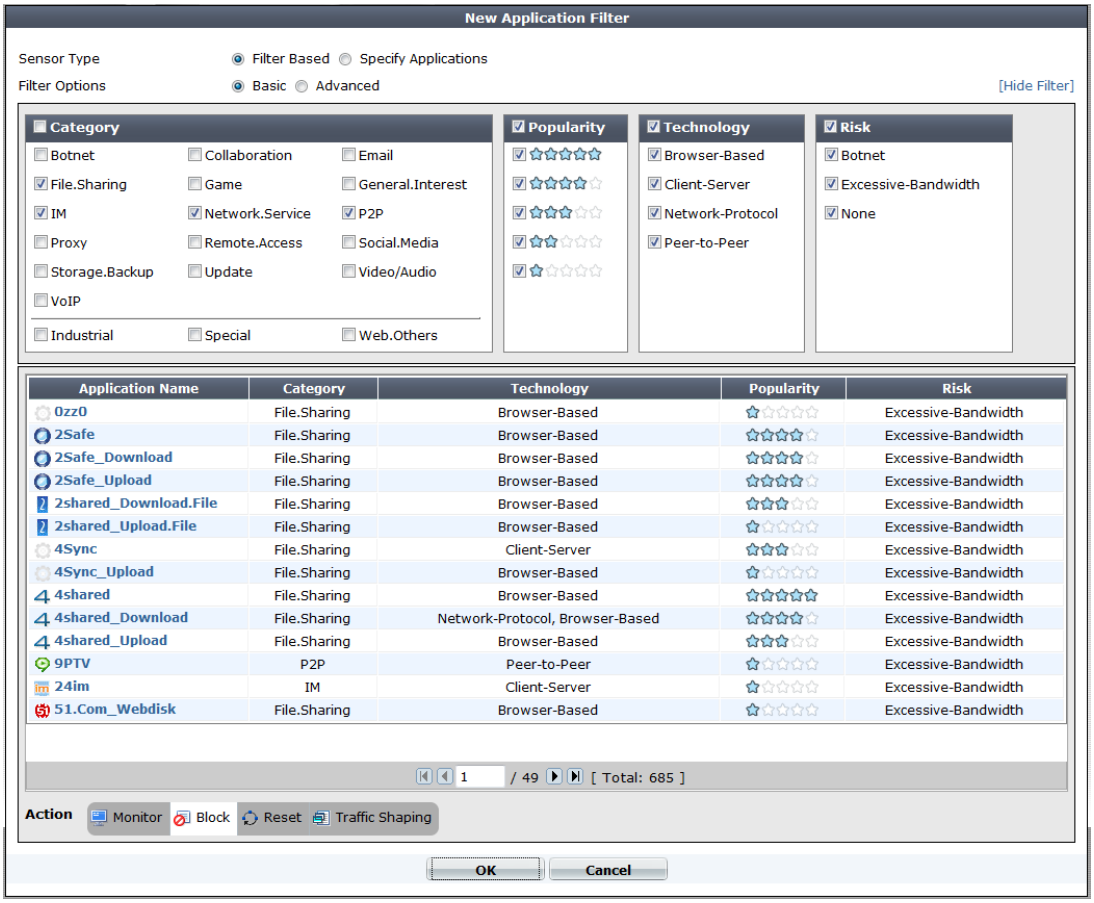
The FortiClient Endpoint Control feature enables the site administrator to distribute an Application Control sensor from a FortiGate device. The process is as follows:

- Create an Application Sensor and Application Filter on the FortiGate
- Add the Application Sensor to the FortiClient Profile on the FortiGate

Step 1: Create a custom Application Control Sensor

1. Login to your FortiGate.
2. In the left tree menu, select *Security Profiles* > *Application Control* > *Application Sensors*.
3. To create a new sensor, click the *Create New* icon (a plus “+” symbol in the upper-right corner).
4. Enter a name for the sensor.
5. Select *OK* to save the sensor.
6. Select *Create Ne*w in the *Edit Application Sensor* toolbar. The *New Application Filter* page opens.

Figure 57: New application filter page



7. In the *Sensor Type* field, select either *Filter Based* or *Specific Applications*.
8. Filter options are available when the *Sensor Type* is *Filter Based*.
9. In the *Category* section, uncheck the check boxes to deselect application categories.
10. In the *Action* section, select *Block*.

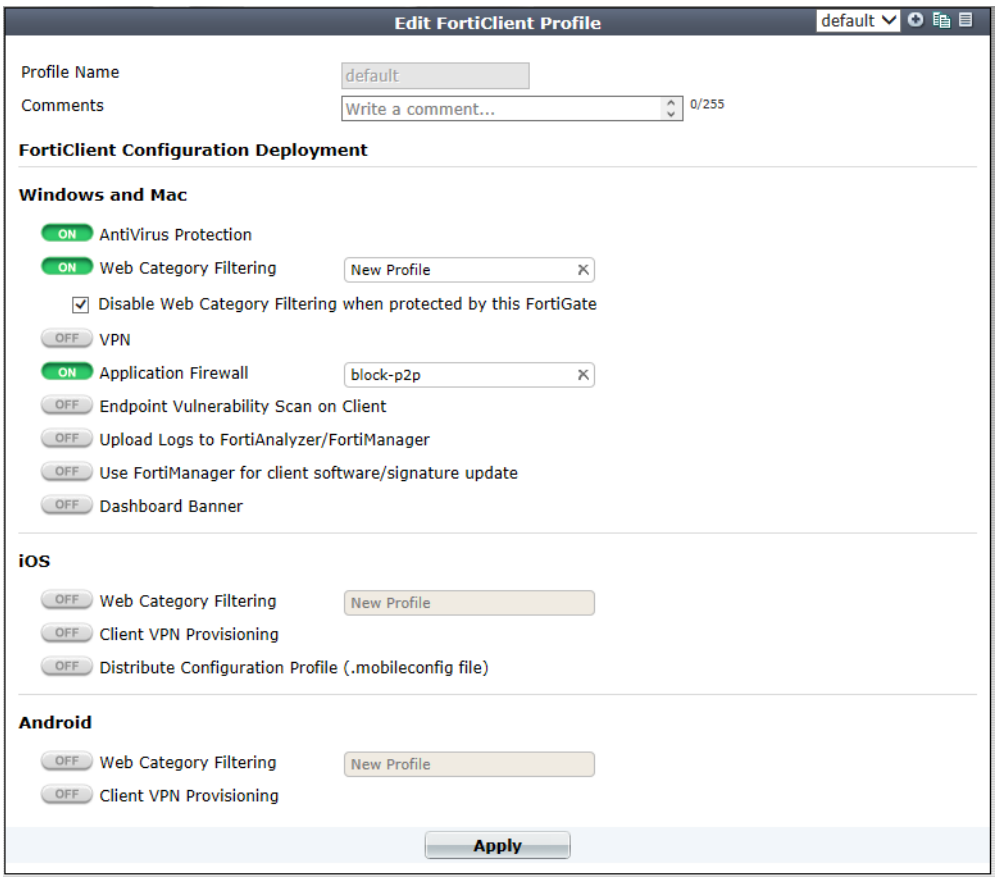
When selecting Monitor or Traffic Shaping, FortiClient will allow the applications selected. When selecting Block or Reset, FortiClient will block the applications selected.

11. Select *OK* to save the profile.

Step 2: Add the Application Control Sensor to the FortiClient Profile

1. In the left tree menu, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
2. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *Application Firewall* button to *ON*.

Figure 58: Edit FortiClient Profile



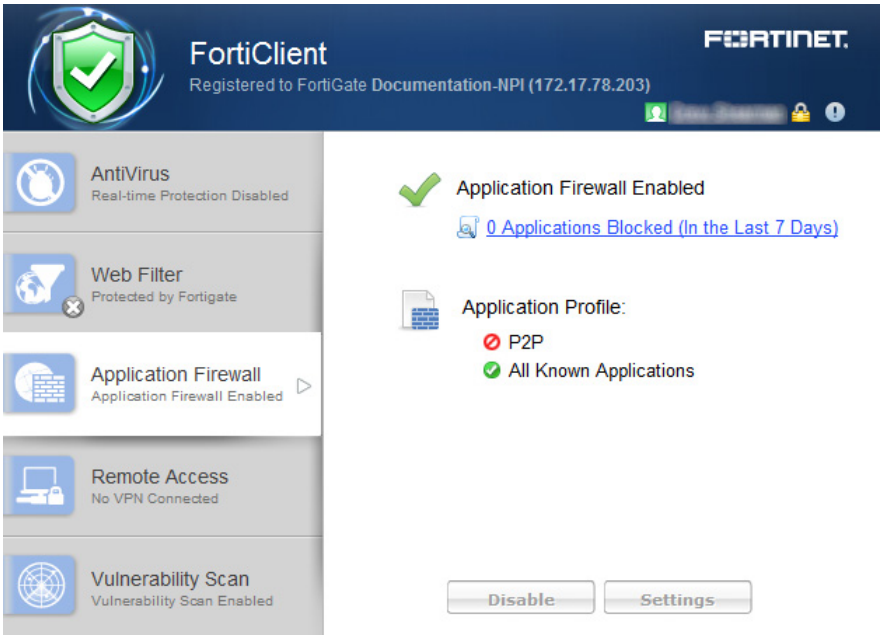
3. Select the Application Sensor in the drop-down list.
4. Select *Apply* to save the profile.

   The FortiGate will send the FortiClient Profile configuration update to registered clients.

Figure 59: Configuration update received by FortiClient

The Application Control module is now available in FortiClient.

Figure 60: Application firewall module



View applications blocked

To view blocked applications, select *Applications Blocked* in the FortiClient console. This page lists all applications blocked in the past seven days, including the count and time of last occurrence.

IPsec VPN and SSL VPN

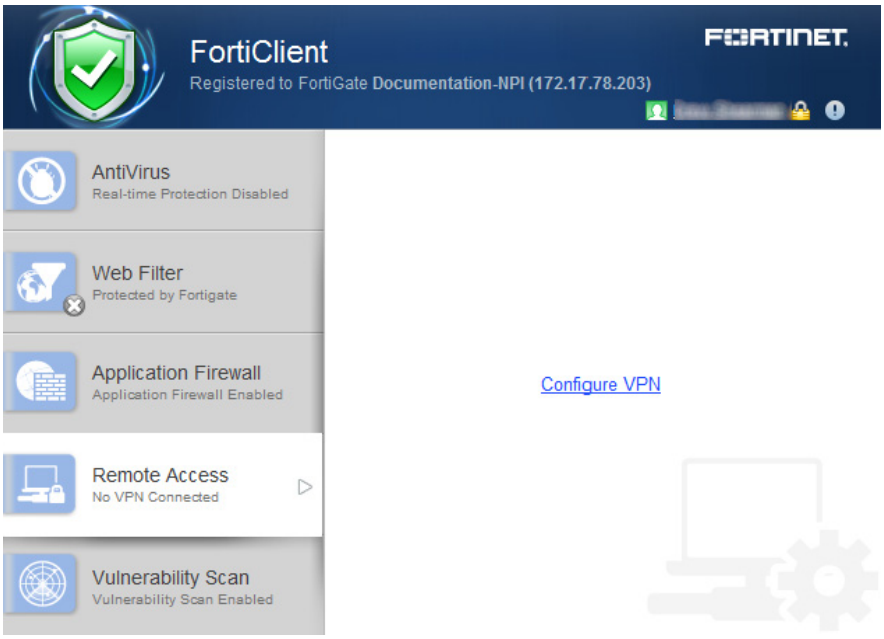
FortiClient version 5.0 supports both IPsec and SSL VPN connections to your network for remote access. You can provision client VPN connections in the FortiClient Profile or configure new connections in the FortiClient console.

This section describes how to configure remote access.

Add a new connection

Select *Configure VPN* in the FortiClient console to add a new VPN configuration.

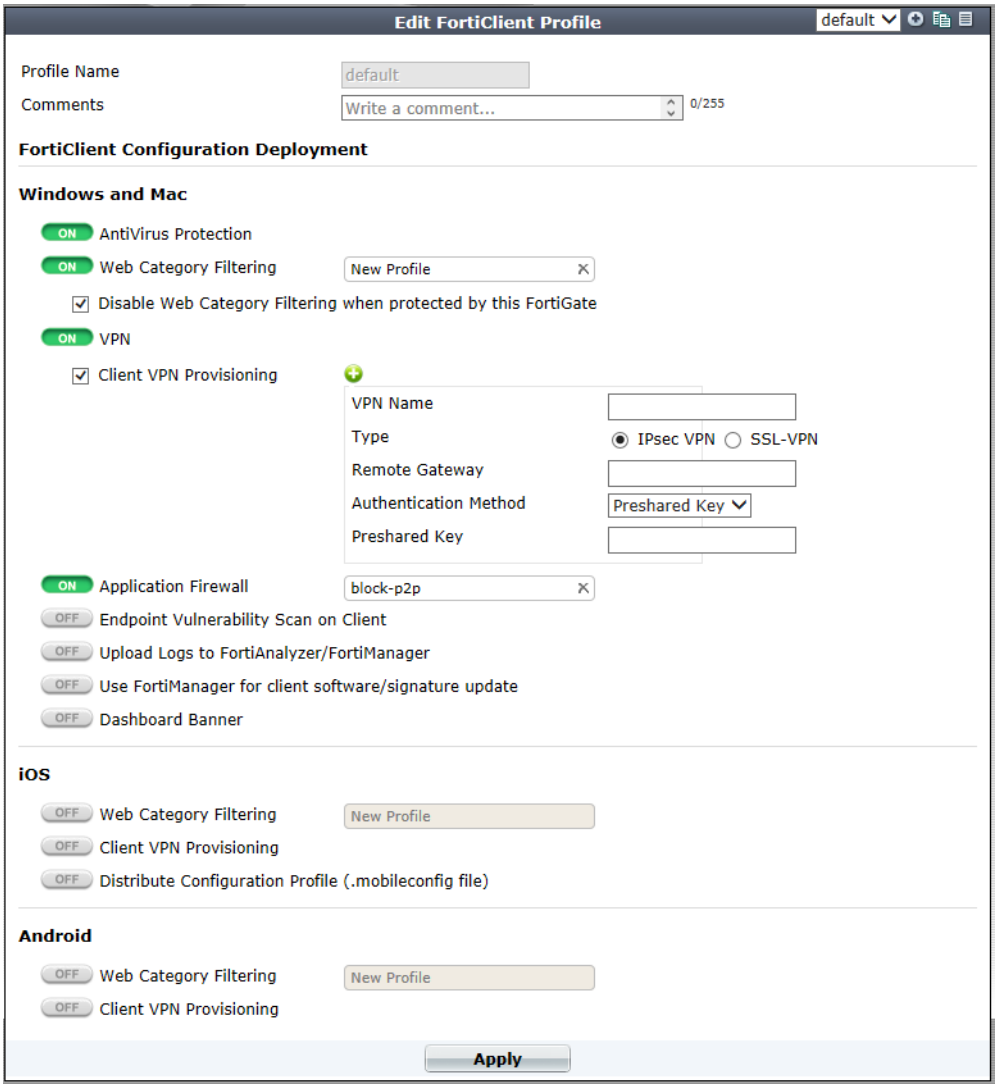
Figure 61: Configure a new VPN connection



Provision a client VPN in the FortiClient Profile:

1. Login to your FortiGate device.
2. In the left tree menu, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
3. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *VPN* button to *ON*.
4. Select the *Client VPN Provisioning* checkbox.
5. Enter a name for the VPN connection.
6. Select the VPN type. Select either *IPsec VPN* or *SSL-VPN*.
7. Configure the remote gateway and authentication settings for the type of VPN selected.

Figure 62: Edit FortiClient Profile



8. Select *Apply* to save the profile.

   The FortiGate will send the FortiClient Profile configuration update to registered clients.

Figure 63: Configuration update received by FortiClient

Figure 64 illustrates VPN settings received by the FortiGate FortiClientprofile. When registered to a FortiGate, VPN settings are enabled and configured in the FortiClient profile.

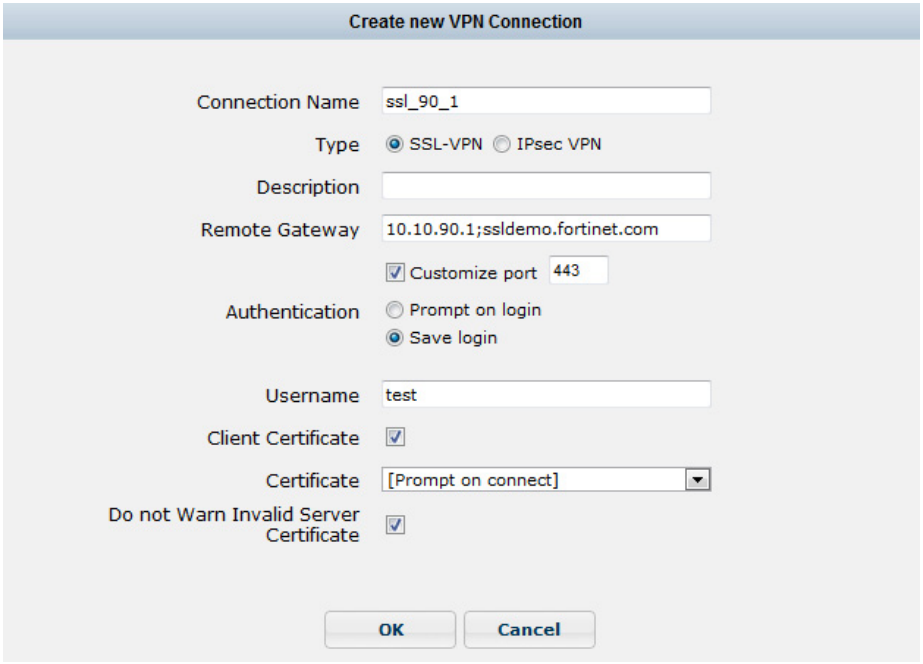
Figure 64:VPN settings in the FortiClient profile

Alternatively, you can provision a client VPN using the advanced VPN FortiClient Profile options in FortiGate. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS 5.0*.

Create a new SSL VPN connection

To create a new SSL VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.

Figure 65:SSL VPN configuration options



Configure the following settings:

Connection Name	Enter a name for the connection.
Type	Select SSL VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Port	Select to change the port. The default port is 443.
Authentication	Select to prompt on login, or save login.
Username	If you selected to save login, enter the username in the dialog box.
Client Certificate	Select to enable client certificates.
Certificate	Select the certificate option in the drop-down menu.
Do not warn Invalid Server Certificate	Select if you do not want to warned if the server presents an invalid certificate.

Create a new IPsec VPN connection

To create a new IPsec VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.

Figure 66:IPsec VPN configuration options

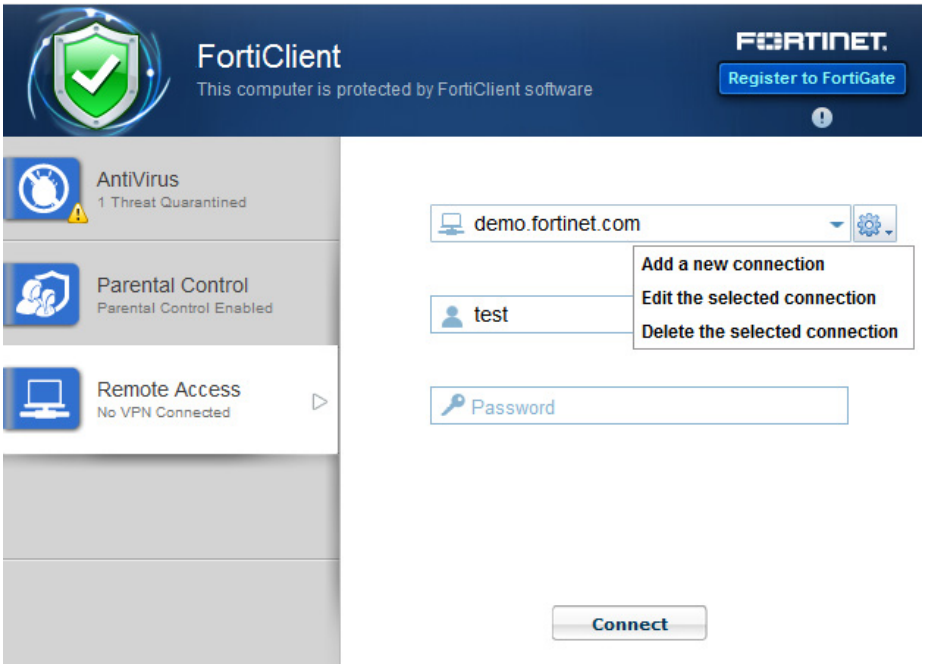
Configure the following settings:

Connection Name	Enter a name for the connection.
Type	Select IPsec VPN.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Authentication Method	Select either *X.509 Certificate* or *Pre-shared Key* in the drop-down menu.
X.509 Certificate, Pre-shared Key	Select *X.509 Certificate* in the drop-down menu, or enter the pre-shared key in the dialog box.
Authentication (XAuth)	Select to prompt on login, save login, or disable.
Username	If you selected save login, enter the username in the dialog box.

Connect to a VPN

To connect to a VPN, select the name of the VPN from the drop-down menu. Enter your username, password, and select the *Connect* button.

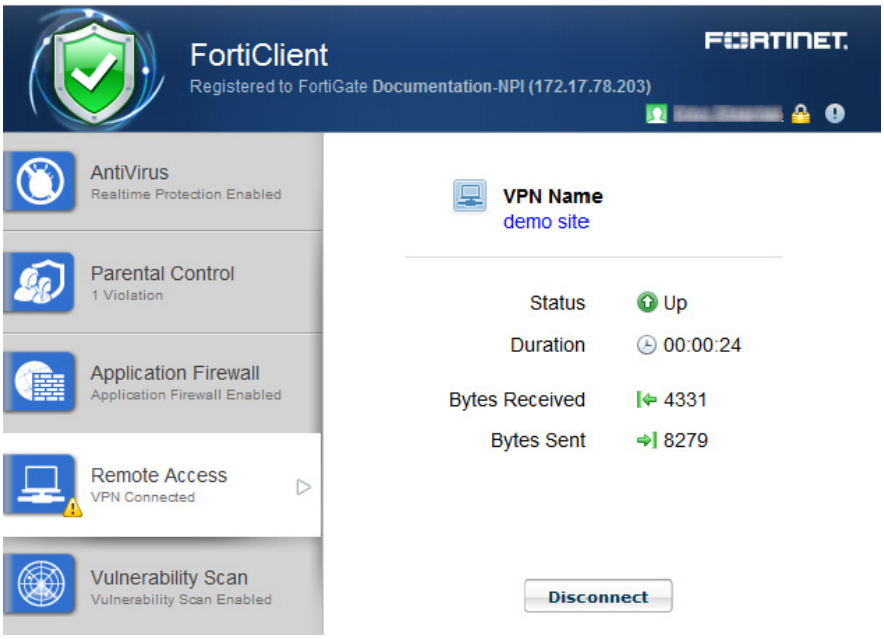
Figure 67: Connection options



You can also select to edit an existing VPN connection and delete an existing VPN connection using the drop-down menu.

When connected, the console will display the connection status, duration, and other relevant information. You can now browse your remote network. Select the *Disconnect* button when you are ready to terminate the VPN session.

Figure 68:SSL VPN connection established



This page displays the following:

Name of the VPN connection	
Status	The status of the VPN connection.
Duration	The duration of the VPN connection.
Bytes Received	Bytes received through the VPN connection.
Bytes Sent	Bytes sent through the VPN connection.
Disconnect	Select to disconnect the VPN connection.

Save Password, Auto Connect, and Always Up (Keep Alive)

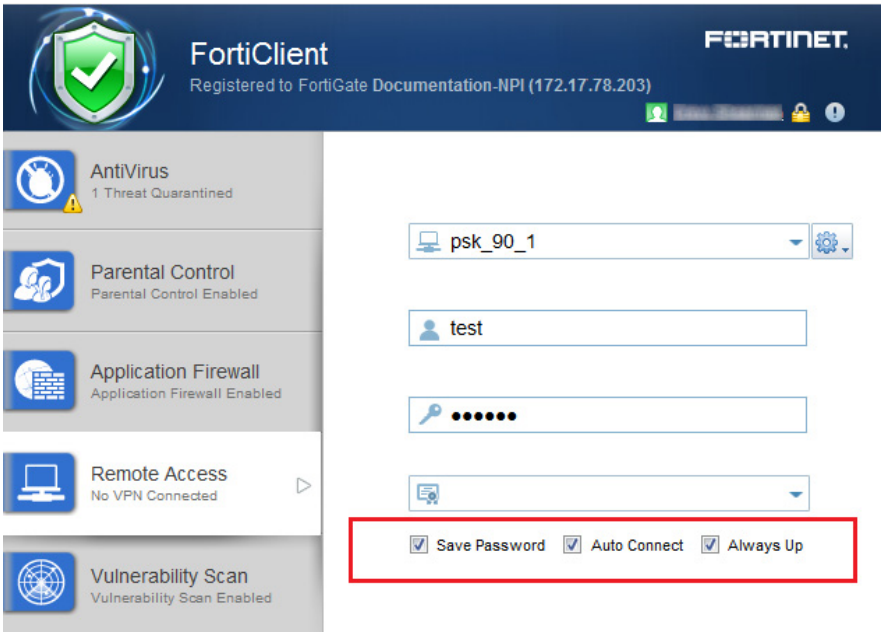
When configuring a FortiClient VPN (IPsec) or SSL VPN connection on your FortiGate device, you can select to enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection will automatically connect.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate will sense when the VPN connection is available and re-connect.

For SSL VPN tunnel mode configurations these features are enabled/disabled in the *SSL VPN Portal*.

When enabled in the FortiGate configuration, once the FortiClient is connected to the FortiGate, the client will receive these configuration options.

Figure 69:IPsec VPN console with features enabled



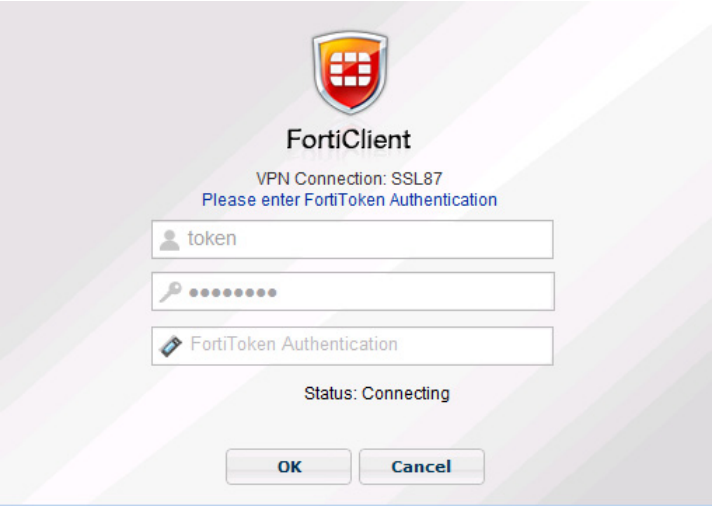
For FortiClient VPN configurations, once these features are enabled they may only be edited from the command line. Use the following FortiOS CLI commands to disable these features:

```
config vpn ipsec phase1-interface
  edit [vpn name]
    set save-password disable
    set client-auto-negotiate disable
    set client-keep-alive disable
  end
end
```

FortiToken and FortiClient VPN

You can use FortiToken with FortiClient for two-factor authentication. See the *FortiOS 5.0 Handbook* for information on configuring FortiToken, user groups, VPN, and two-factor authentication on your FortiGate device for FortiClient VPN connections.

Figure 70: FortiToken authentication



Advanced features (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Activating VPN before Windows Logon

When using VPN before Windows logon, the user is offered a list of pre-configured VPN connections to select from in the Windows logon screen. This requires that the Windows logon screen is not bypassed. As such, if VPN before Windows logon is enabled, it is required to also check the check box *Users must enter a user name and password to use this computer* in the *User Accounts* dialog box.

To make this change, proceed as follows:

In FortiClient,

1. Create the VPN tunnels of interest or use Endpoint Control to register to a FortiGate which provides the VPN list of interest
2. Enable VPN before logon in the FortiClient Settings page.

In the Windows system,

1. Start an elevated command line prompt.
2. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
3. Check the check box for *Users must enter a user name and password to use this computer*.
4. Click *OK* to save the setting.

Connect VPN before logon (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
  <vpn>
    <options>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
    </options>
  </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
```

```
            </options>
               <connections>
                  <connection>
                     <name>psk_90_1</name>
                     <type>manual</type>
                     <ike_settings>
                     <prompt_certificate>0</prompt_certificate>
                     <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                          .143</server>
                     <redundantsortmethod>1</redundantsortmethod>
                     ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
                    3</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Advanced features (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                  .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

VPN tunnel & script (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on FortiGate's XML format FortiClient Profile. The profile will be pushed down to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>windows</os>
      <script>
        <script>
          <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Ted Mosby
md c:\test
copy x:\PDF\*.* c:\test
                ]]>
        </script>
      </script>
  </on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
net use x: /DELETE
            ]]>
</script>
      </script>
    </script>
  </on_disconnect>
```

VPN tunnel & script (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>mac</os>
    <script>
      /bin/mkdir /Volumes/installers
      /sbin/ping -c 4 192.168.1.147 >
           /Users/admin/Desktop/dropbox/p.txt
      /sbin/mount -t smbfs
           //kimberly:RigUpTown@ssldemo.fortinet.com/installer
           s /Volumes/installers/ >
           /Users/admin/Desktop/dropbox/m.txt
      /bin/mkdir /Users/admin/Desktop/dropbox/dir
      /bin/cp /Volumes/installers/*.log
           /Users/admin/Desktop/dropbox/dir/.
    </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>mac</os>
    <script>
      /sbin/umount /Volumes/installers
      /bin/rm -fr /Users/admin/Desktop/dropbox/*
  </script>
  </script>
</on_disconnect>
```

Vulnerability Scan

FortiClient version 5.0 includes an *Vulnerability Scan* module to check your personal computer for known system vulnerabilities.

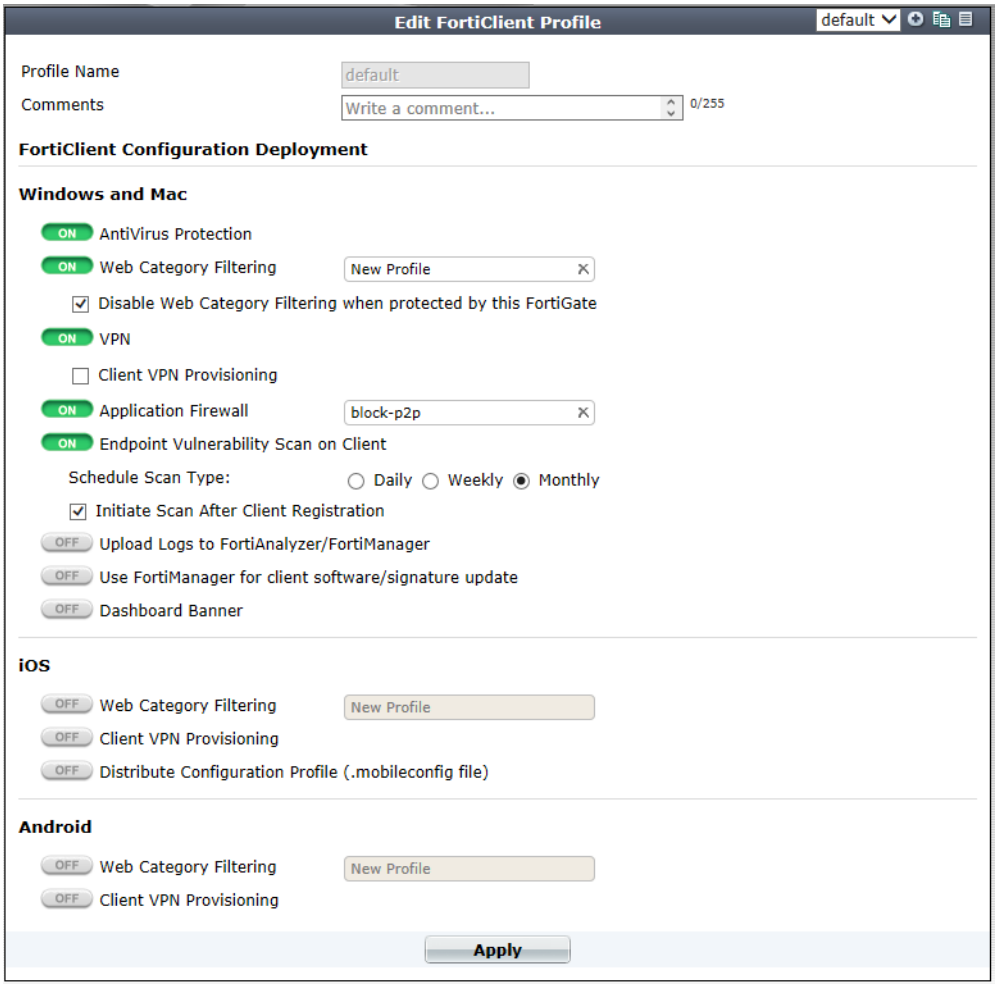
In FortiClient version 5.0.4 or later, this feature is disabled by default and the tab is hidden for standalone clients. For uses who are registered to a FortiGate using endpoint control, the FortiGate administer may choose to enable this feature.

This section describes how to enable *Vulnerability Scan* in the FortiGate FortiClient profile and configuration options.

Enable Vulnerability Scan in the FortiClient Profile:

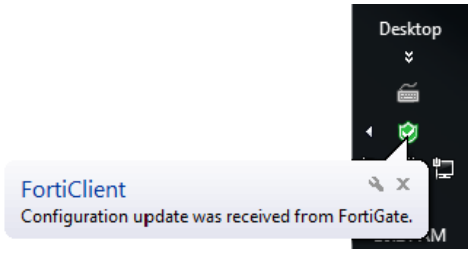
1. Login to your FortiGate device.
2. In the left tree menu, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
3. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *Endpoint Vulnerability Scan on Client* button to *ON*.
4. Select the schedule scan type. Select one of: *Daily*, *Weekly*, or *Monthly*.
5. Select the checkbox to *Initiate Scan After Client Registration*.

Figure 71: Edit FortiClient Profile



6. Select *Apply* to save the profile.
   The FortiGate will send the FortiClient Profile configuration update to registered clients.

Figure 72: Configuration update was received from FortiGate



The Vulnerability Scan module is now available in FortiClient.

Figure 73: Vulnerability scan page

Scan now

To perform a vulnerability scan, select the *Scan Now* button in the FortiClient console. FortiClient will scan your personal computer for known vulnerabilities. The console displays the date of the last scan above the button.

Update now

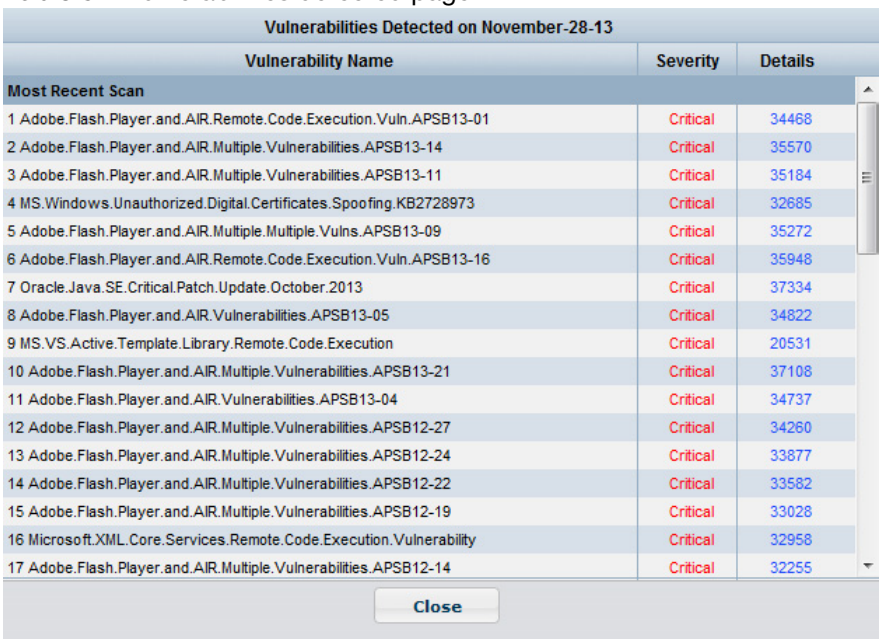
Select the *Update Now* button in the FortiClient console to update the vulnerability signature.

You can select to use a FortiManager device for client software and signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

View vulnerabilities

When the scan is complete, FortiClient will display the number of vulnerabilities found in the FortiClient console. Select the *Found* link to view a list of vulnerabilities detected on your system.

Table 5: Vulnerabilities detected page

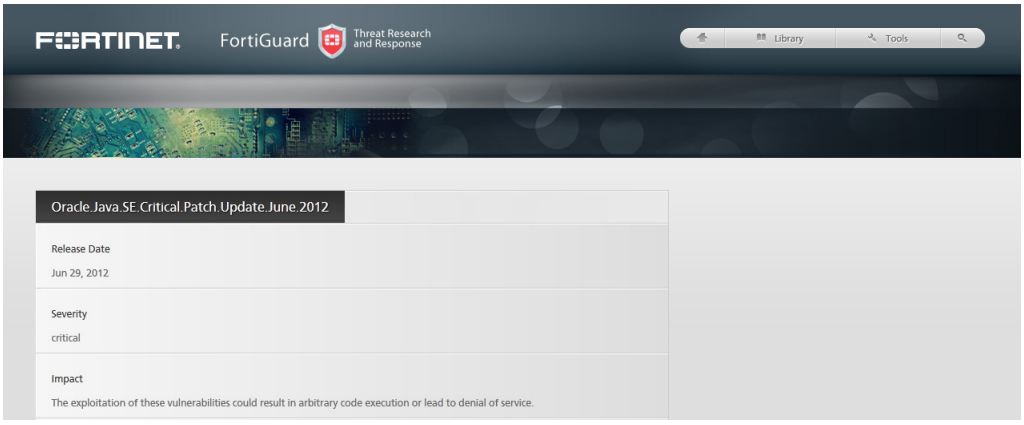


This page displays the following:

Vulnerability Name	The name of the vulnerability
Severity	The severity level assigned to the vulnerability; Critical, High, Medium, Low, Info.
Details	FortiClient vulnerability scan lists a Bugtraq (BID) number under the details column. You can select the BID to view details of the vulnerability in the FortiGuard site, or search the web using this BID number.
Close	Close the window and return to the FortiClient console.
Clear	Clear the Vulnerability Scan results.

Select the *Details* ID number from the list to view information for the selected vulnerability in the FortiGuard site. The site details the release date, severity, impact, description, affected products, and recommended actions.

Figure 74: FortiGuard site details



Vulnerability scan logging

To configure Vulnerability Scan logging, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. Select *Vulnerability Scan* in the logging menu to enable logging for this module.

Vulnerability scan logging is disabled while you are registered to a FortiGate.

Settings

This sections describe the available option in the settings menu.

For registered clients, the following controls in the settings page are available:

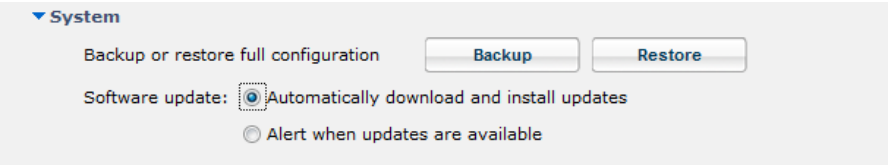
- System
  - Backup
- Logging
  - Export logs
- Advanced
  - Disable configuration sync with FortiGate

    By disabling this option, this client will be considered as non-compliant and your network traffic might be blocked by FortiGate.
  - Disable proxy (troubleshooting only)

Backup or restore full configuration

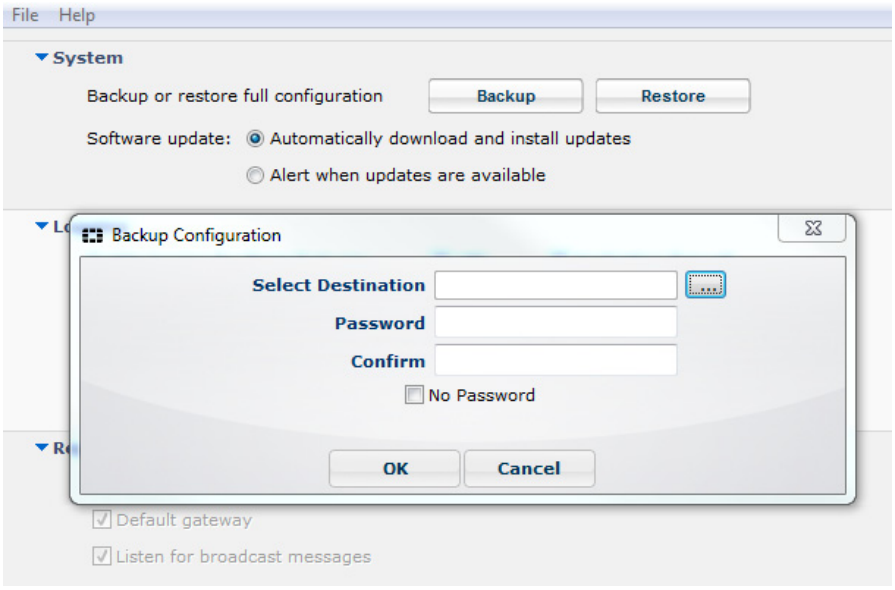
To backup or restore the full configuration file select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can perform a backup or restore a full configuration file.

Figure 75: Backup and restore options



When performing a backup you can select the file destination and save the file in an unencrypted or encrypted format.

Figure 76: Backup configuration dialog box



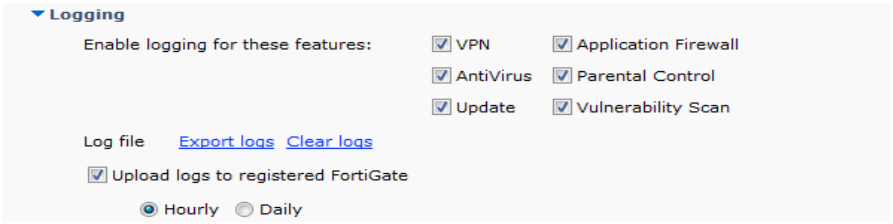
Logging

To configure logging, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. In this menu you can configure logging for the following features:

- VPN
- Antivirus
- Update
- Application Firewall
- Parental Control
- Vulnerability Scan

You can specify the logging level and select to export logs or clear logs.

Figure 77: Logging options



The following table lists the logging levels and description:

Table 6: FortiClient logging levels

Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.

Table 6: FortiClient logging levels (continued)

Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

FortiClient can be configured via the endpoint profile to send traffic, vulnerability scan, and event logs to your FortiAnalyzer or FortiManager device running v5.0.2 or later.

Configure logging to FortiAnalyzer or FortiManager

To configure FortiClient to log to your FortiAnalyzer or FortiManager you require the following:

- FortiClient version 5.0.2 or later
- A FortiGate device running FortiOS version 5.0.2 or later
- A FortiAnalyzer or FortiManager device running version 5.0.2 or later

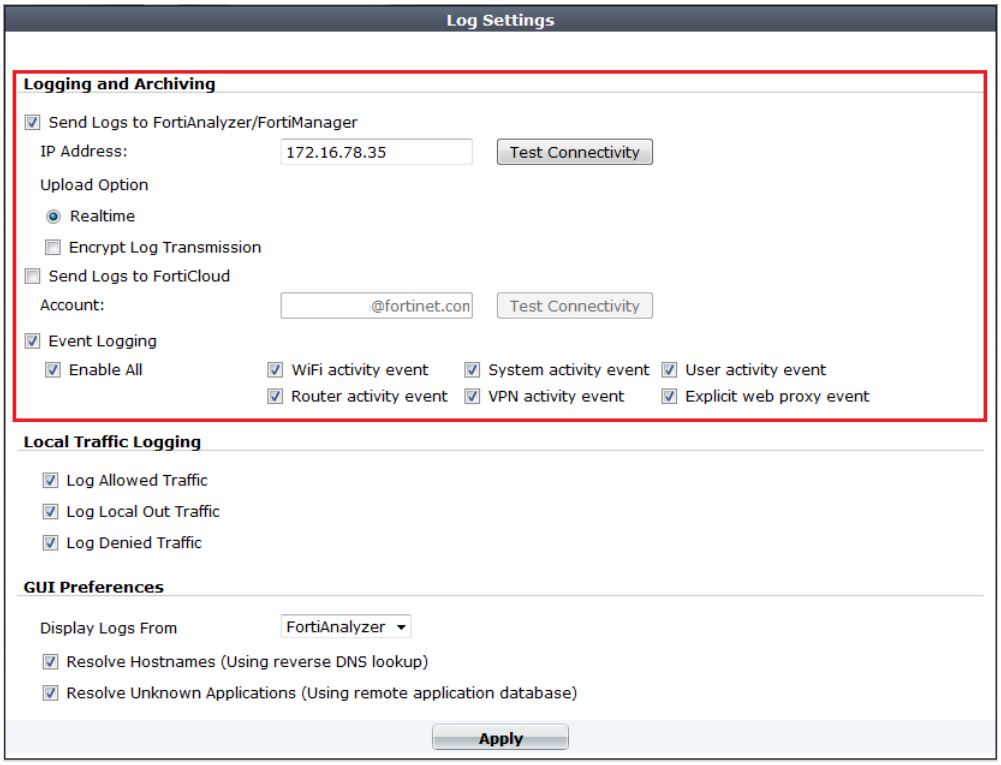
The registered FortiClient device will send traffic logs, vulnerability scan logs, and event logs to the log device on port 514 TCP.

FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.

Enable logging on the FortiGate device:

1. On your FortiGate device, select *Log & Report* > *Log Config* > *Log Settings*. The *Log Settings* window opens.

Figure 78: Log settings window

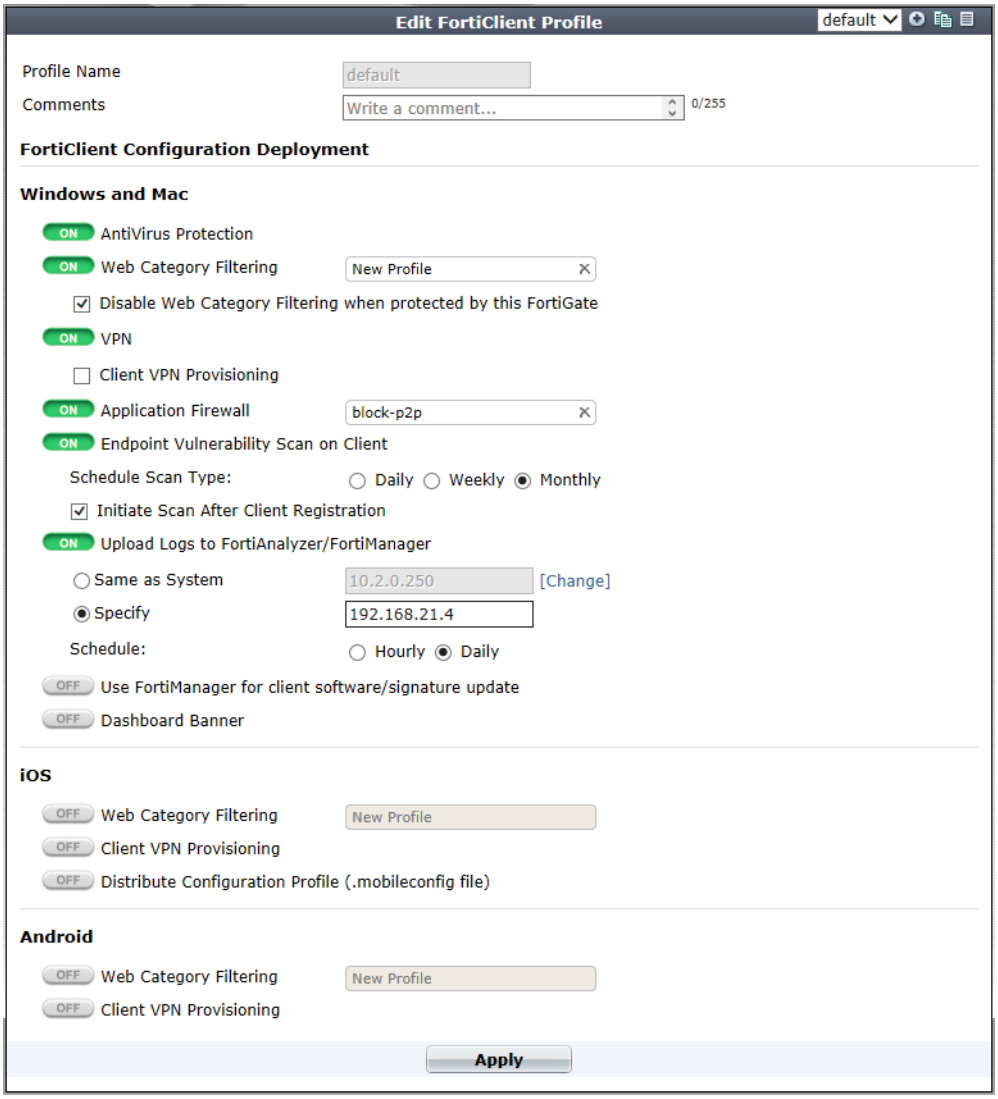


2. Select the *Send Logs to FortiAnalyzer/FortiManager* checkbox to enable this feature. Enter the IP address of your log device. You can select *Test Connectivity* to ensure your FortiGate is able to communicate with the log device on this IP address.
3. Select *Apply* to save the setting.

FortiClient must be able to access the FortiAnalyzer/FortiManager IP address in order to forward logs.

4. Select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. The *Edit FortiClient Profile* window opens.

Figure 79: Edit FortiClient Profile



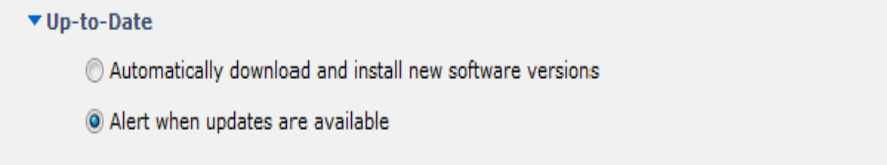
5. Under *FortiClient Configuration Deployment Windows and Mac*, toggle the *Upload Logs to FortiAnalyzer/FortiManager* feature to *ON*. You can select either *Same as System* which will follow the FortiGate settings or *Specify* to enter a different IP address. Under *Schedule*, select to upload logs *Hourly* or *Daily*. Selecting *Change* beside the IP address text box will re-direct you to the Log settings window.
6. Select *Apply* to save the setting. Once the FortiClient Profile change is synchronized with the client, you will start receiving logs from registered clients on your FortiAnalyzer/FortiManager system.

   To download the FortiClient log files in the FortiAnalyzer go to the *Log View* tab, select the ADOM, and select the *FortiClient* menu object.

Updates

To configure updates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can configure the behavior of FortiClient when a new software version is available on the FortiGuard Distribution Servers (FDS).

Figure 80: Update options



You can select to use a FortiManager device for client software and signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

To configure FortiClient to use FortiManager for software and signature updates:

1. On your FortiOS device, select *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.
2. Toggle the *Use FortiManager for client software/signature update* option to *ON*.
3. Specify the IP address of the FortiManager to use for client software and signature updates.
4. Select the checkbox beside *Failover to FDN when FortiManager is not available* to have FortiClient receive updates from the FortiGuard Distribution Network when the FortiManager is not available to ensure your clients are always protected.
5. Select *Apply* to save the setting.

VPN options

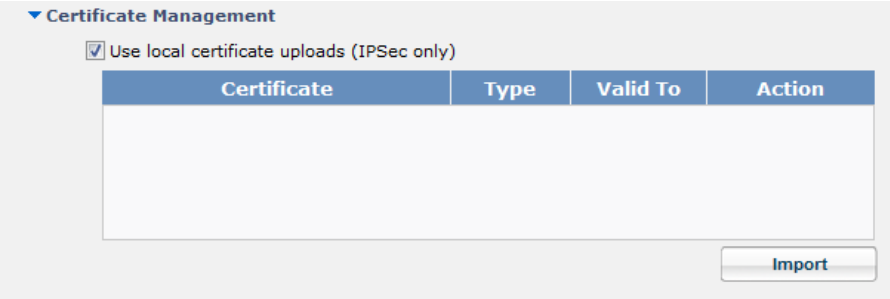
To configure VPN options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *VPN Options* to view the drop-down menu. In this menu you can configure to enable VPN before logon.

Figure 81:VPN options

Certificate management

To configure VPN certificates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Certificate Management* to view the drop-down menu. In this menu you can configure IPsec VPN to use local certificates and import certificates to FortiClient.

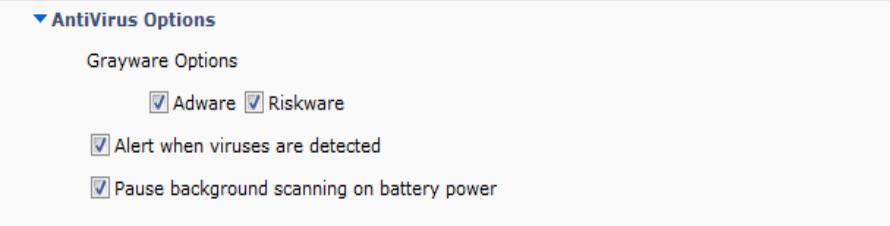
Figure 82: Certificate management options



Antivirus options

To configure antivirus options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure grayware options and the behavior of FortiClient when a virus is detected.

Figure 83: Antivirus options



Configure the following settings:

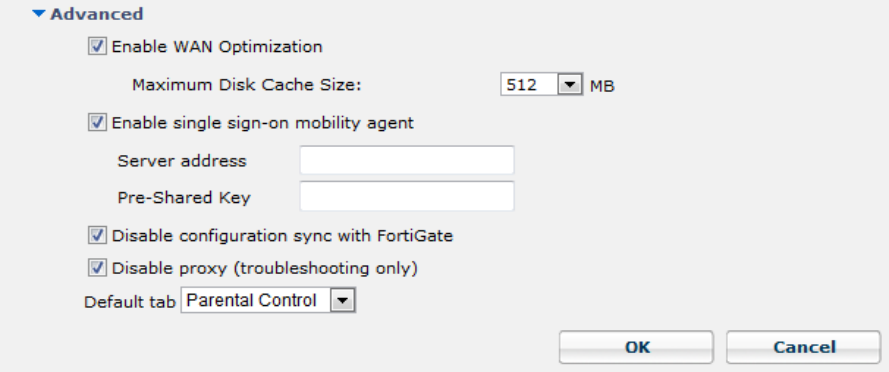
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Alert when viruses are detected	Select to display notification message window when a virus is detected.

Pause background scanning on battery power	Select to pause background scanning when on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Advanced options

To configure advanced options, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Advanced* to view the drop-down menu. In this menu you can configure WAN Optimization, Single Sign-On, configuration sync with FortiGate, disable proxy, and the default tab when FortiClient is started.

Figure 84: Advanced options



Configure the following settings:

Advanced	Advanced FortiClient settings.
Enable WAN Optimization	Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization.
Maximum Disk Cache Size	Select to configure the maximum disk cache size. The default value is 512MB.
Enable Single Sign-On mobility agent	Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
Server address	Enter the FortiAuthenticator IP address.
Customize port	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
Disable configuration sync with FortiGate	Select to disable configuration synchronization with FortiGate. By disabling this option, this client will be considered as non-compliant and your network traffic might be blocked by FortiGate.

Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient.
Default tab	Select the default tab to be displayed when opening FortiClient.

Single Sign-On (SSO) mobility agent

The FortiClient Single Sign-On Mobility Agent acts as a client that updates with FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator protocol

The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- The FortiAuthenticator should be accessible from clients in all locations.
- The FortiAuthenticator should be accessible by all FortiGates.

FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running version 2.0.0 or later, or version 3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator.

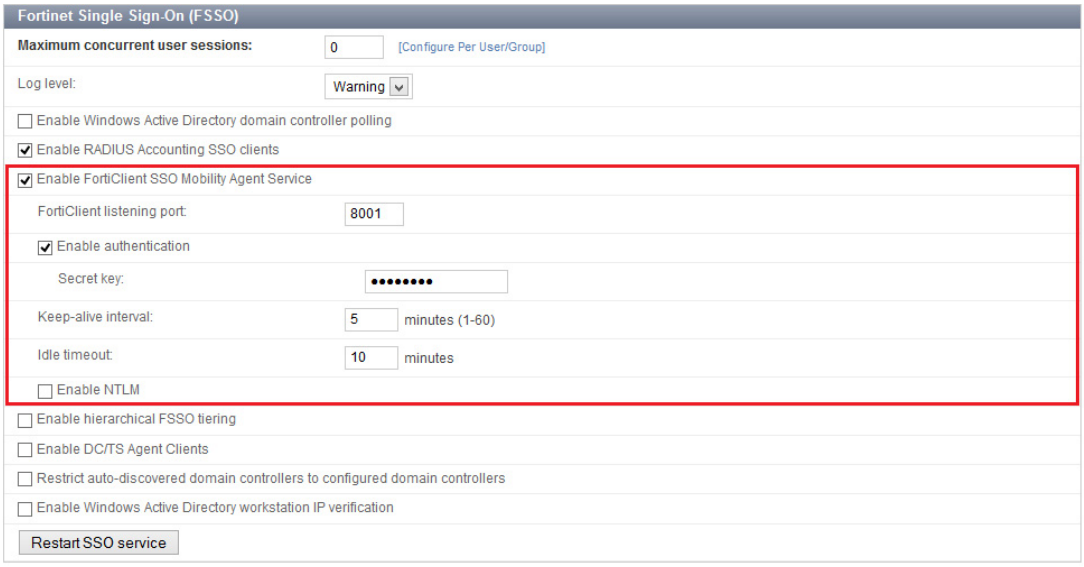
Enable Single Sign-On mobility agent on FortiClient:

1. Select *File* in the toolbar and select *Settings* in the drop-down menu.
2. Select *Advanced* to view the drop-down menu.
3. Select to *Enable Single Sign-On mobility agent*.
4. Enter the FortiAuthenticator server address and the pre-shared key.

Enable FortiClient SSO mobility agent service on the FortiAuthenticator:

1. Select *Fortinet SSO Methods* > *SSO* > *General*. The *Edit SSO Configuration* page opens.

Figure 85: FortiAuthenticator configuration window

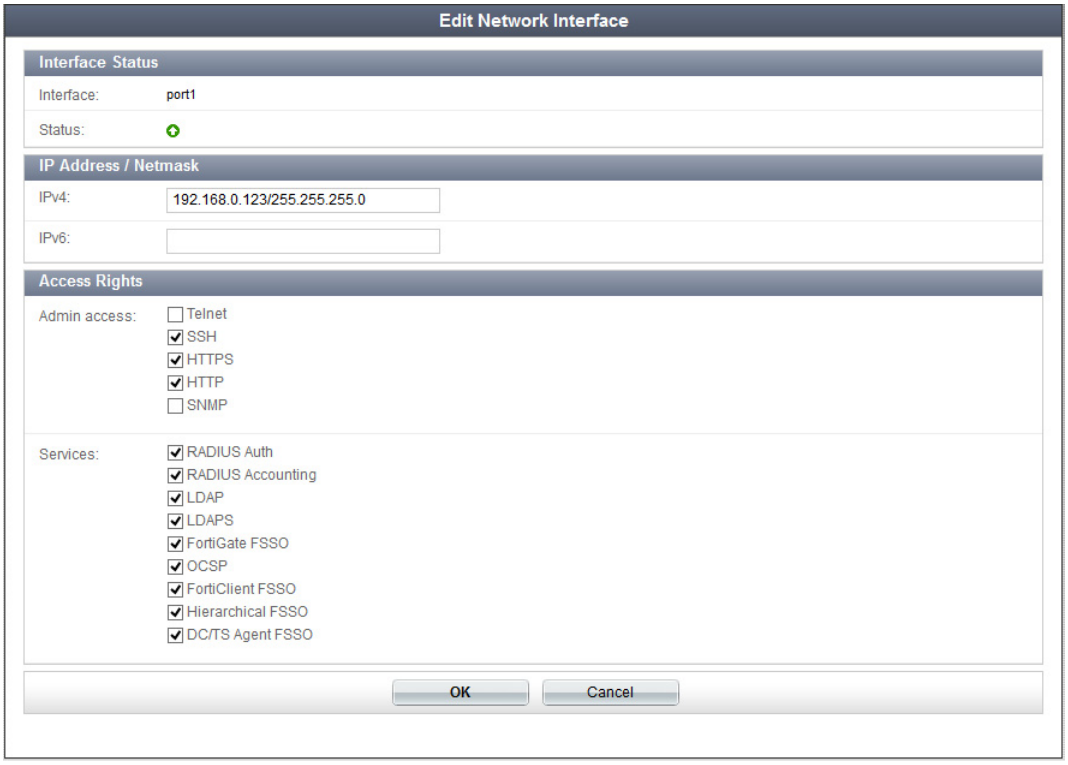


2. Select *Enable FortiClient SSO Mobility Agent Service* and a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret-key value.
4. Select *OK* to save the setting.

To enable FortiClient FSSO services on the interface:

1. Select *System* > *Network* > *Interfaces*. Select the interface and select Edit from the toolbar. The *Edit Network Interface* window opens.

Figure 86: Edit network interface window



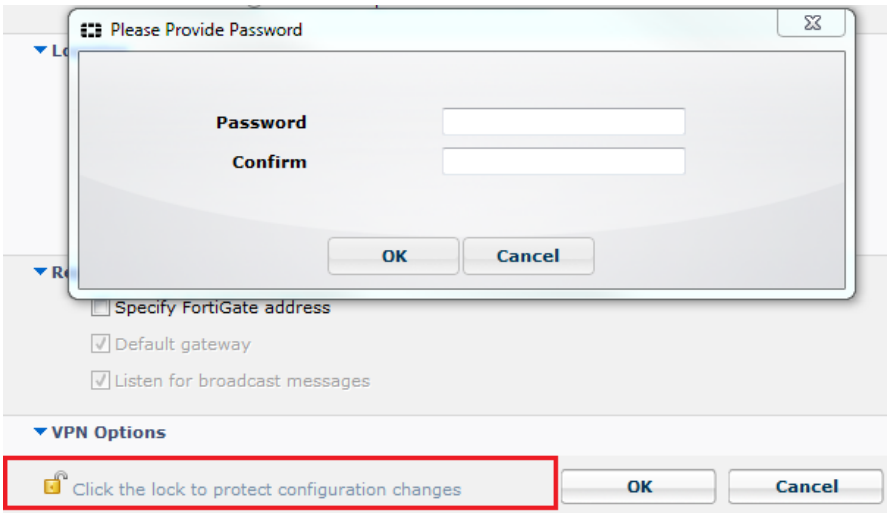
2. Select the checkbox to enable *FortiClient FSSO*.
3. Select *OK* to save the setting.

To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator Administration Guide* at http://docs.fortinet.com. For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller.

Configuration lock

To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the *Settings* page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

Figure 87: Configuration lock window and dialog box



When the configuration is locked you can perform the following actions:

- Antivirus
  - Complete an antivirus scan, view threats found, and view logs
  - Select *Update Now* to update signatures
- Parental Control
  - View violations
- Application Firewall
  - View applications blocked
- Remote Access
  - Configure, edit, or delete an IPsec VPN or SSL VPN connection
  - Connect to a VPN connection
- Vulnerability Scan
  - Complete a vulnerability scan of the system
  - View vulnerabilities found
- Register and unregister FortiClient for Endpoint Control

- Settings
  - Export FortiClient logs
  - Backup the FortiClient configuration

To perform configuration changes or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration.

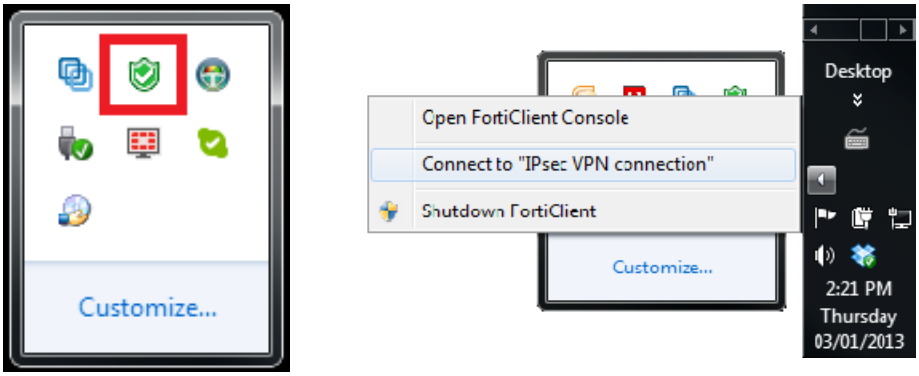
FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient console is closed.

- Default menu options
  - Open FortiClient console
  - Shutdown FortiClient
- Dynamic menu options depending on configuration
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

Figure 88: System tray icon and FortiTray menu



When the configuration is locked, the option to shut down FortiClient from FortiTray is greyed out.

Connect to a VPN connection

To connect to a VPN connection from FortiTray, select the Windows System Tray and right-click in the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, and select *OK* to connect.

Figure 89: Authentication window

Custom FortiClient Installations

The FortiClient Configurator tool (Microsoft Windows) and FortiClient Repackager tool (Mac OS X) are the recommended methods of creating customized FortiClient installation files.

This document was written for FortiClient (Windows) v5.0.10. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0.10.

You can also customize which modules are displayed in the FortiClient dashboard in the FortiClient Profile. This will allow you to activate any of the modules at a later date without needing to re-install FortiClient. Any changes made to the FortiClient Profile are pushed to registered clients.

When creating VPN only installation files, you cannot enable other modules in the FortiClient Profile as only the VPN module is installed.

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClientProfile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

The FortiClient Configurator/FortiClient Repackager tool is included with the FortiClient Tools file in FortiClient v5.0.5 or later. This file is only available in the Customer Service & Support portal and is located in the same file directory as the FortiClient images.

The Configurator/Repackager tool requires activation with a license key each time it is used. Ensure that you have completed the following steps prior to logging in to your FortiCare product web portal:

- Purchased FortiClient Registration License
- Activated the FortiClient license on a FortiGate

This video explains how to purchase and apply a FortiClient License:
http://www.youtube.com/watch?feature=player_embedded&v=sIkWaUXK0Ok

This chapter contains the following sections:

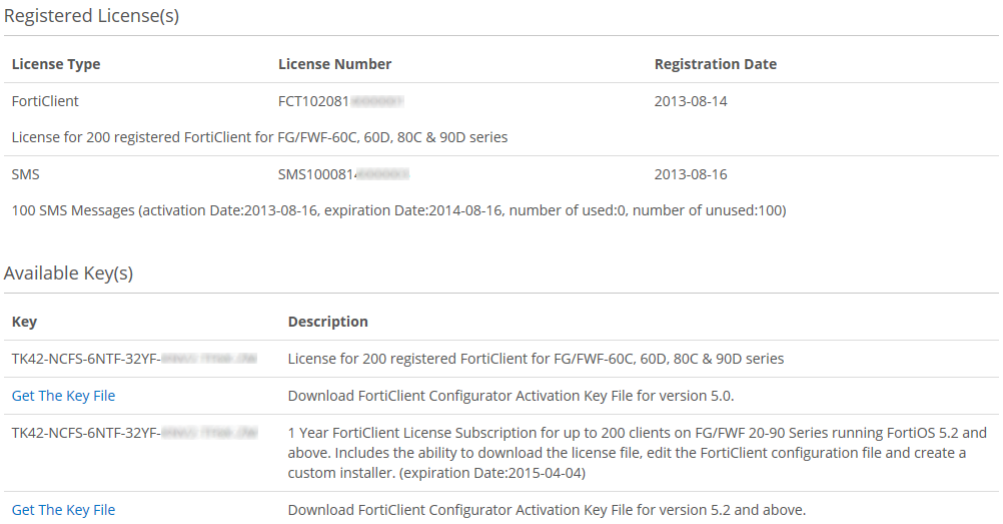
Download the license file (activation key file)

To retrieve your license file:

1. Go to https://support.fortinet.com and login to your FortiCare account.
2. Under *Asset* select *Manage/View Products*. Select the FortiGate device that has the FortiClient registration license activated.

   You will see the *Get The Key File* link in the *Available Key(s)* section.

   Figure 90: FortiClient licenses



Registered License(s)

License Type	License Number	Registration Date
FortiClient	FCT102081	2013-08-14
License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series		
SMS	SMS100081	2013-08-16
100 SMS Messages (activation Date:2013-08-16, expiration Date:2014-08-16, number of used:0, number of unused:100)		

Available Key(s)

Key	Description
TK42-NCFS-6NTF-32YF-	License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.0.
TK42-NCFS-6NTF-32YF-	1 Year FortiClient License Subscription for up to 200 clients on FG/FWF 20-90 Series running FortiOS 5.2 and above. Includes the ability to download the license file, edit the FortiClient configuration file and create a custom installer. (expiration Date:2015-04-04)
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.2 and above.

3. Click the link and download license file to your management computer. This file will be needed each time you use the Configurator/Repackager tool.

Activate the Configurator/Repackager tool

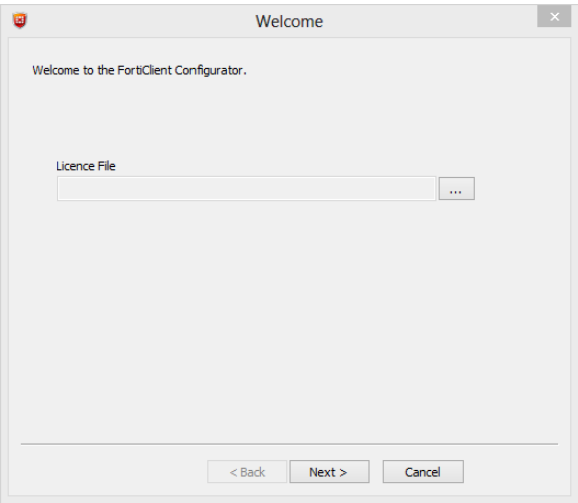
Fortinet offers a repacking tool for both Microsoft Windows and Mac OS X operating systems.

FortiClient (Windows) Configurator tool

To activate the FortiClient Configurator tool:

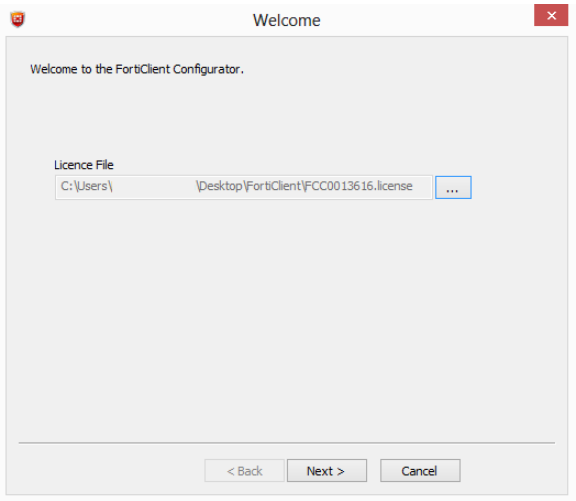
1. Unzip the FortiClientTools file, select the FortiClientConfigurator file folder, and double-click the *FortiClientConfiguratorGUI.exe* application file to launch the tool. The tool opens at the *Welcome* page.

Figure 91: Configurator tool



2. Browse and select the FortiClient Configurator Activation Key file (.license) on your management computer.

Figure 92: License file selected



3. Select *Next*.

   The tool will now be activated and ready to use.

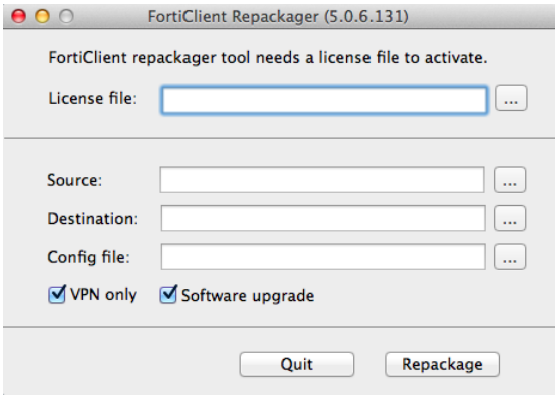
Since the FortiClient Configurator tool is not installed in the management computer, you must upload the FortiClient Configurator Activation Key file (.license) each time you run the tool.

FortiClient (Mac OS X) Repackager tool

To activate the FortiClient Repackager tool:

1. Unzip the FortiClientTools file, select the Repackager file folder, and double-click the *FortiClientRepackager.dmg* application file, and double-click the FCTRepackager icon to launch the tool. The *Repackager* tool opens.

Figure 93: FortiClient Repackager tool



2. Browse and select the FortiClient Configurator Activation Key file (.license) on your management computer.

   You can now continue to use the tool.

Create a custom installer

In FortiClient v5.0.10, three options are available for custom installations:

- A VPN only installation file: will only install VPN features (IPSec VPN/SSL VPN), either with or without preconfigured settings.
- A full installation file (Antivirus, Web Filtering, VPN, Application Firewall, Vulnerability Scan) with or without preconfigured settings.
- Disable software updates.

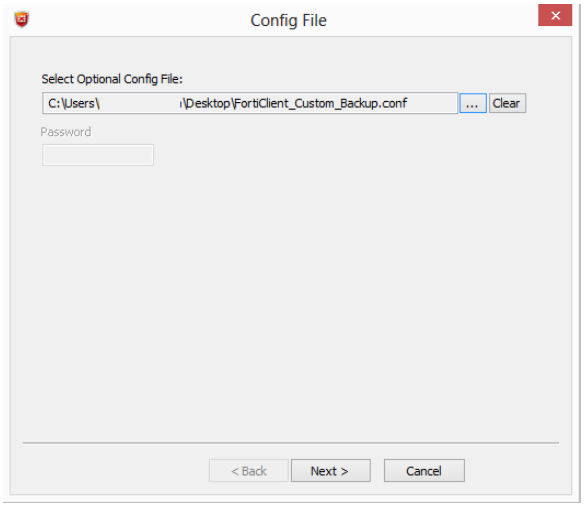
To include preconfigured FortiClient settings in your custom installer, the FortiClient configuration XML file can be selected. If the backup file is encrypted, enter the password in the text field.

You can use an XML editor to make changes to the FortiClient configuration file. For more information on FortiClient XML configuration, see the *FortiClient v5.0.10 XML Reference* at the Fortinet Technical documentation site, http://docs.fortinet.com.

FortiClient (Windows) Configurator tool

After entering the FortiClient Configurator license, select Next. If preconfigured settings are not required, select *Skip*.

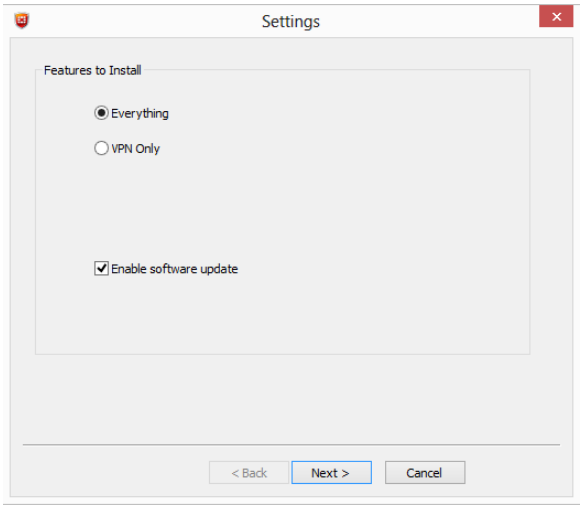
Figure 94: Optional configuration file



Select the installation type in the *Settings* page. On this page you can select to install everything or VPN only. You can also enable or disable software updates.

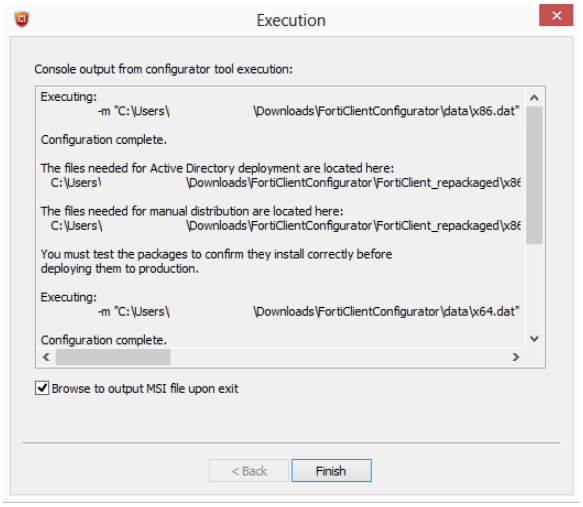
When selecting to install VPN only, all other modules are not installed. To enable these features you will need to uninstall FortiClient, and reinstall an MSI file with these features enabled.

Figure 95: Select the custom installation type



Select *Next* to proceed to the *Execution* page. This page provides details of the MSI file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

Figure 96: Finish the custom installer creation



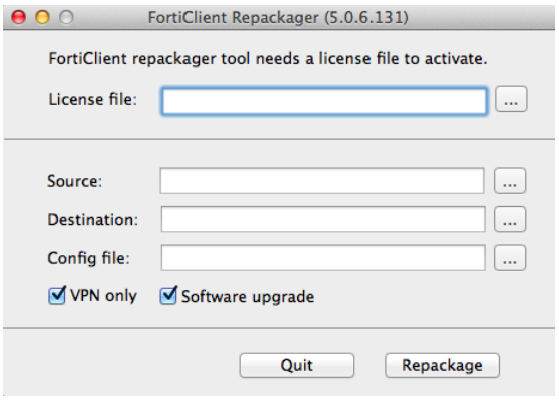
When you select *Finish*, if *Browse to output MSI file upon exit* is selected, the folder containing the newly created MSI file will open.

Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly.

FortiClient (Mac OS X) Repackager tool

After entering the FortiClient Configurator license you can continue to create a custom FortiClient installation file.

Figure 97: FortiClient Repackager Tool

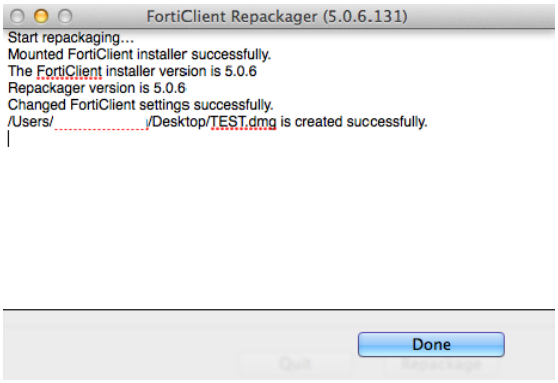


Configure the following settings:

License File	Enter the FortiClient Configurator license key.
Source	Select the FortiClient Installer file on your management computer. Note: You must use the full installer file, otherwise FortiClient Repackager will fail to create a custom installation file. Note: The FortiClient Installer version and FortiClient Repackager version must match, otherwise the Repackager will fail to create a custom installation file.
Destination	Enter a name for the custom installation file and select a destination to save the file on your management computer.
Config file	Optionally, select a pre-configured FortiClient backup configuration file.
VPN only	Select to install the VPN module only. All other modules will not be installed.
Software upgrade	Select to enable or disable software upgrades/updates.

Select the *Repackage* button to create the custom FortiClient installation file.

Figure 98: Start repackaging



You can now deploy the repackaged FortiClient .dmg file to your Mac OS X systems.

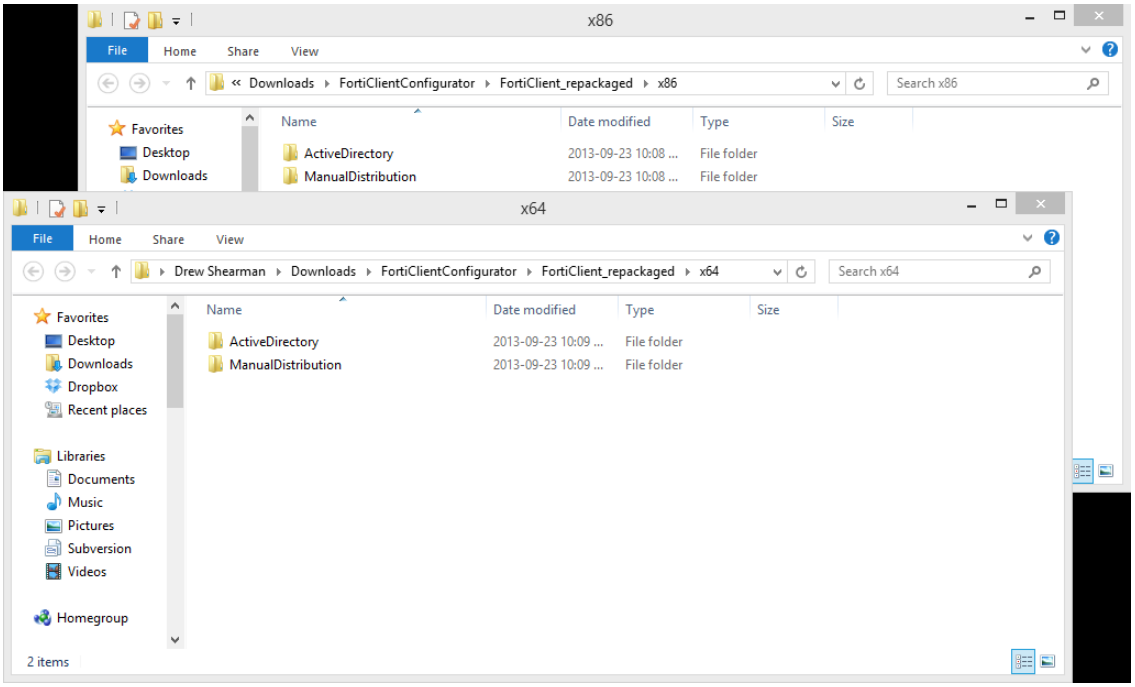
Custom installation packages

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.0.10 XML Reference* and the *CLI Reference for FortiOS 5.0*.

FortiClient (Windows)

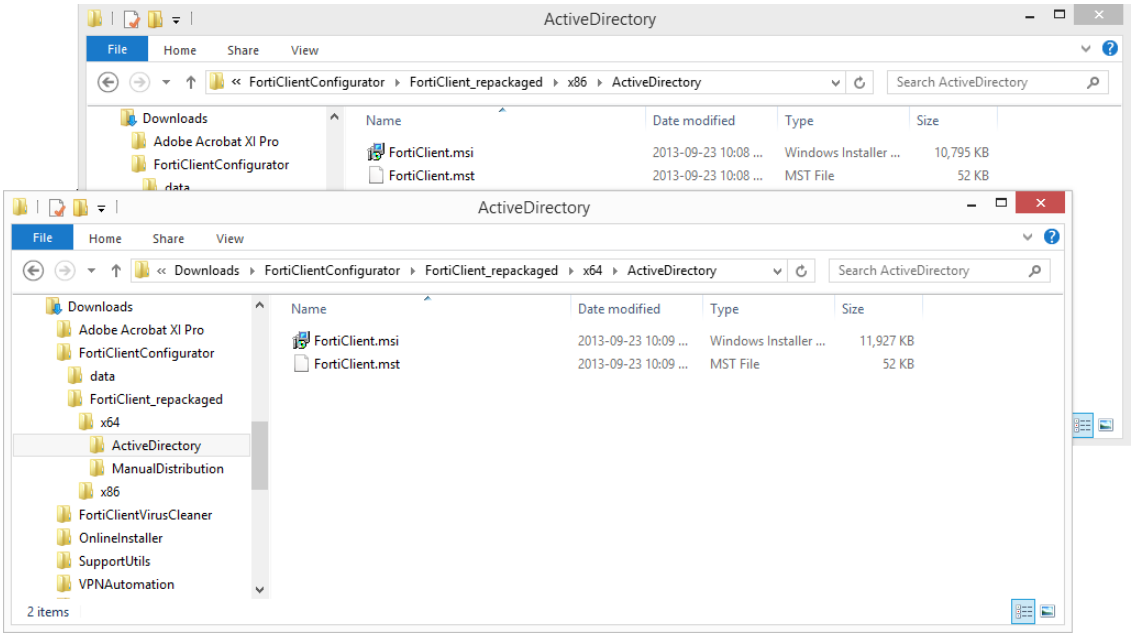
After the configurator tool generates the custom installation packages, it can be used to deploy the FortiClient software either manually, or using Active Directory. Both options can be found in the *.../FortiClient_packaged* directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

Figure 99: FortiClient_packaged folder



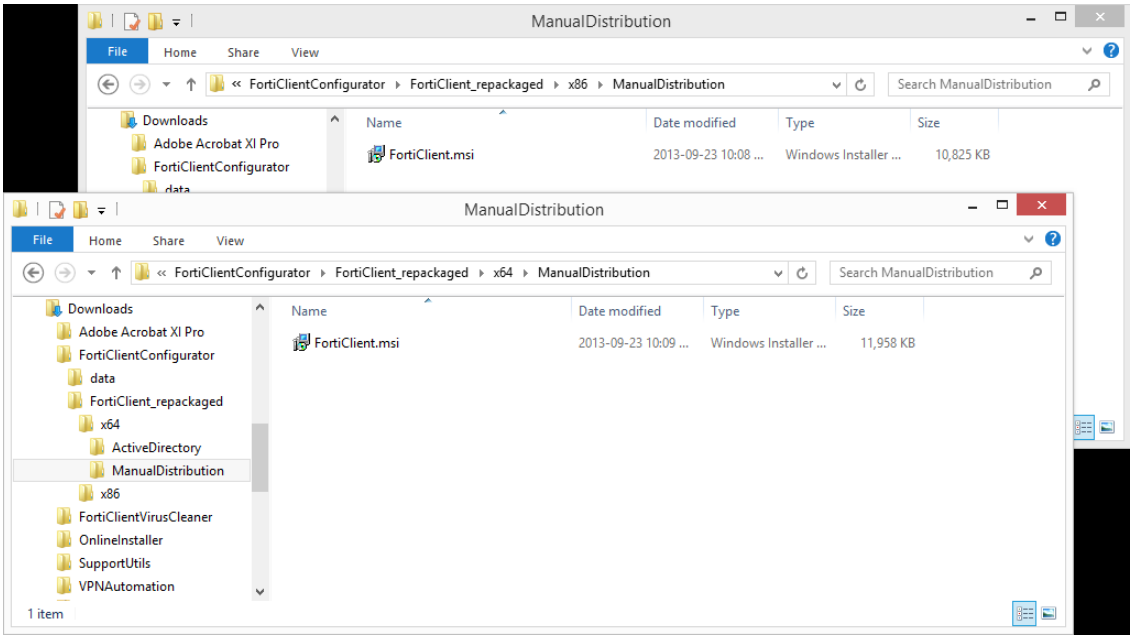
If Active Directory is being used to deploy FortiClient, you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

Figure 100: ActiveDirectory folder



For manual distribution, use the MSI file in the *.../ManualDistribution* folder.

Figure 101: ManualDistribution folder



Advanced FortiClient profiles

When creating custom FortiClient MSI files for deployment, you will need to configure advanced FortiClient profiles on the FortiGate to ensure that settings in the FortiClient profile do not overwrite your custom XML settings. You can configure the FortiClient profile to deliver the full XML configuration, VPN only, or specific FortiClient XML configurations. For more information on customizing the FortiClient XML configuration file, see the FortiClient v5.0.10 XML Reference.

Fortinet recommends creating OS specific endpoint profiles when provisioning XML settings. When creating a new FortiClient profile, select the device group as either Windows PC or Mac. If a FortiClient (Windows) XML configuration is pushed to a FortiClient (Mac OS X) system, FortiClient (Mac OS X) will ignore settings which are not supported.

Provision a full XML configuration file

To deploy the full XML configuration via the FortiClient Profile:

1. Log in to the FortiGate Command-line Interface.
2. Enter the following CLI commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
    set forticlient-advanced-cfg-buffer "Copy & Paste your
        FortiClient XML configuration here"
  end
end
```

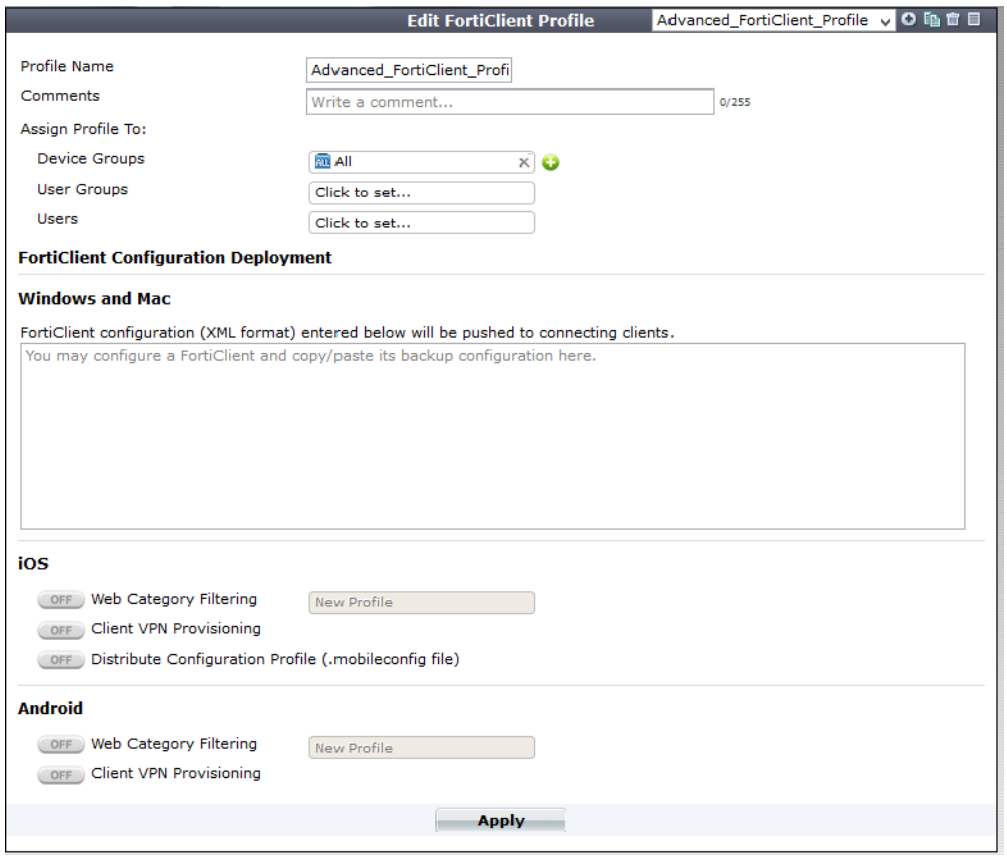
After `forticlient-advanced-cfg` is enabled, the `forticlient-advanced-cfg-buffer` CLI command is available from the CLI.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<?xml version="1.0" encoding="UTF-8" ?>` start of syntax to the `</forticlient_configuration>` end of syntax XML tags. Add double quotes at the start and end of the XML syntax statements.

The buffer size for the FortiClient Control XML configuration is 32kB.

You can also choose to copy & paste the XML content in the Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles.*

Figure 102: Advanced FortiClient Control profile



Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient profile.
Comments	Optionally, enter a comment.
Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS 5.0 Handbook*. Note: These options are only available when creating a new FortiClient profile. Note: You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN. Note: FortiClient does not support nested groups in FortiOS.
Device Groups	Select device groups from the drop down-menu. Use the add icon to select more than one device group.
User Groups	Select user groups from the drop-down menu. Use the add icon to select more than one device group.
Users	Select users from the drop-down menu. Use the add icon to select more than one device group.

FortiClient Configuration Deployment Windows and Mac	
XML text window	Cut and paste the FortiClient XML configuration file in the text window. The XML syntax must be preserved.

Select *Apply* to save the FortiClient profile settings.

The current buffer size is 32kB. This may not be large enough to accommodate your FortiClient XML configuration. As a workaround, you can use the FortiClient Configurator tool to create a custom MSI installation file using a `.conf` FortiClient backup configuration that contains static custom configurations. You can then include a partial configuration in the advanced FortiClient profile. This will push the partial configuration when the client registers with the FortiGate. The partial configuration will be merged with the existing XML configuration on the client.

To provision specific FortiClient XML configuration while preserving custom XML configurations in your MSI file, cut & paste the specific XML configuration into the FortiClient Profile in the following format:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
  <system>
    <ui>
      <ads>0</ads>
      <default_tab>VPN</default_tab>
      <flashing_system_tray_icon>0</flashing_system_tray_icon>
      <hide_system_tray_icon>0</hide_system_tray_icon>
      <suppress_admin_prompt>0</suppress_admin_prompt>
      <culture_code>os-default</culture_code>
    </ui>
    <update>
      <use_custom_server>0</use_custom_server>
      <port>80</port>
      <timeout>60</timeout>
      <failoverport>8000</failoverport>
      <fail_over_to_fdn>1</fail_over_to_fdn>
      <scheduled_update>
        <enabled>0</enabled>
        <type>interval</type>
        <daily_at>03:00</daily_at>
        <update_interval_in_hours>3</update_interval_in_hours>
    </scheduled_update>
    </update>
  </system>
</forticlient_configuration>
```

Ensure that the `<partial_configuration>1</partial_configuration>` tag is set to 1 to indicate that this partial configuration will be deployed upon registration with the FortiGate. All other XML configuration will be preserved.

Advanced VPN provisioning

You need to enable VPN provisioning and advanced VPN from the FortiOS CLI to import the FortiClient XML VPN configuration syntax. You can import the XML VPN configuration in the CLI or the Web-based Manager.

Import XML VPN configuration into the FortiClient Profile via the CLI:

1. Log in to your FortiGate command-line interface.
2. Enter the following CLI commands:

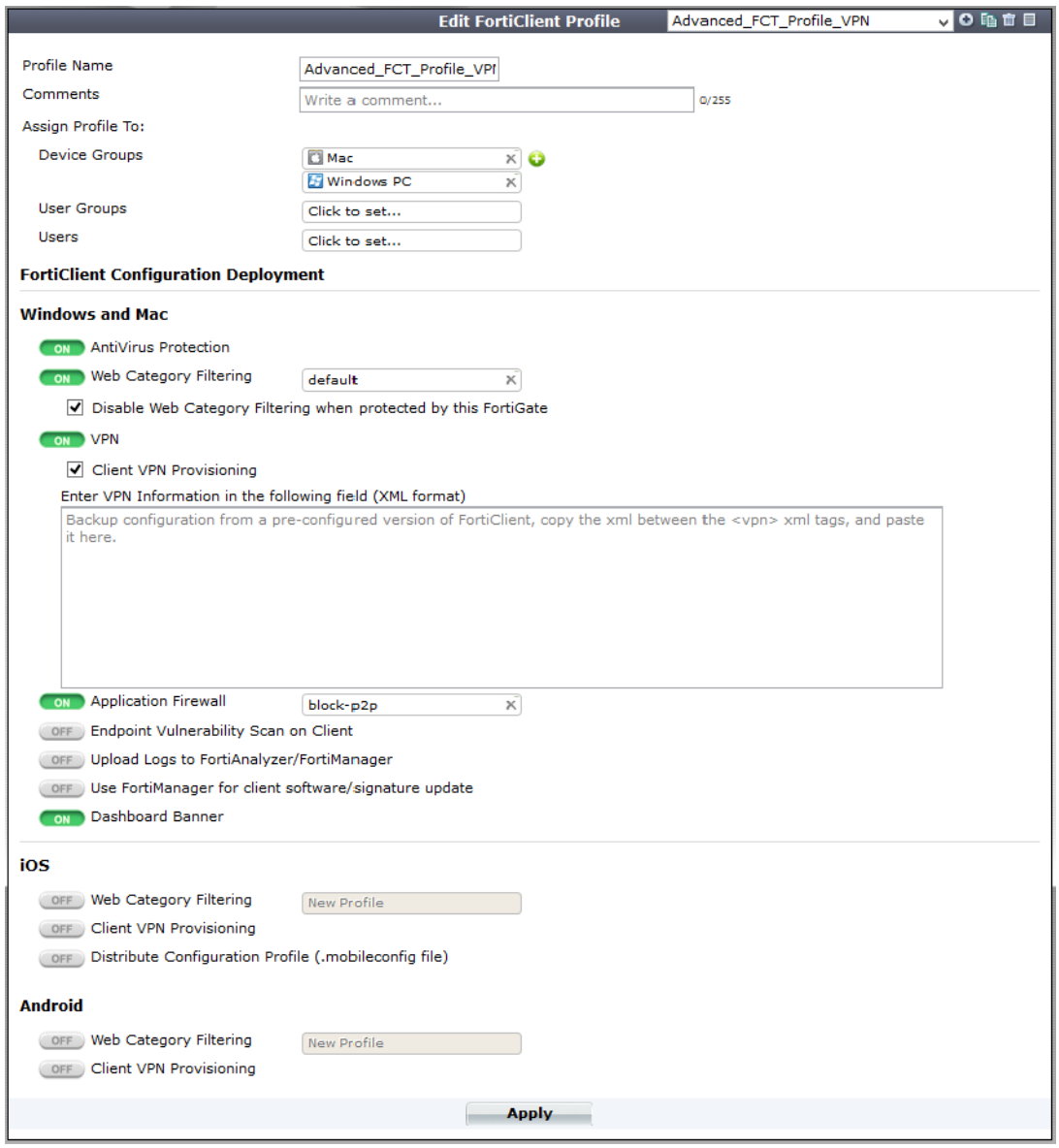
```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-vpn-provisioning enable
    set forticlient-advanced-vpn enable
    set forticlient-advanced-vpn-buffer "Copy & paste the
        advanced VPN configuration"
  end
end
```

After the `forticlient-vpn-provisioning` and `forticlient-advanced-vpn` CLI commands are enabled, the `forticlient-advanced-vpn-buffer` CLI command is available from the CLI.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<vpn>` start of syntax to the `</vpn>` end of syntax XML tags. Add double quotes before the `<vpn>` tag and after the `</vpn>` tag.

You can also choose to copy & paste the XML content in the Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles.*

Figure 103: Advanced FortiClient profile (VPN)



Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient profile.
Comments	Optionally, enter a comment.
Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS 5.0 Handbook*. Note: These options are only available when creating a new endpoint profile. Note: You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN. Note: FortiClient does not support nested groups in FortiOS.

Device Groups	Select device groups from the drop down-menu. Use the add icon to select more than one device group.
User Groups	Select user groups from the drop-down menu. Use the add icon to select more than one device group.
Users	Select users from the drop-down menu. Use the add icon to select more than one device group.
FortiClient Configuration Deployment Windows and Mac	
AntiVirus Protection	Toggle the button on or off to enable or disable this feature.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.
VPN	Select the checkbox for Client VPN Provisioning. Cut and paste the FortiClient XML configuration `<vpn>` to `</vpn>` tags in the text window. The XML syntax must be preserved.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down menu.
Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select Specify to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address.
Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.
Dashboard Banner	Toggle the button on or off to enable or disable this feature.

Select *Apply* to save the FortiClient profile settings.

Upgrade Information

FortiClient (Windows) v5.0.10 upgrade information

Please review the *FortiClient (Windows) v5.0.10 Release Notes* prior to upgrading your client. The following information outlines supported upgrade paths and methods.

When upgrading on a Windows XP system, a warning dialog box is displayed indicating that one of the files to be updated is currently in use. Please select the `Ignore` button to continue with the upgrade.

Users with newer Windows OS versions will receive a different warning dialog box. It warns that a reboot will be required to complete the installation. Please click the *OK* button to continue with the installation.

Upgrading from FortiClient version 5.0.0

FortiClient v5.0.10 supports direct upgrade from FortiClient version 5.0.0 or later, along with the regular manual upgrade method.

Upgrading from FortiClient Lite version 4.3

FortiClient v5.0.10 supports manual upgrade from FortiClient Lite version 4.3.5.

Upgrading from FortiClient Connect version 4.3

FortiClient v5.0.10 supports manual upgrade from FortiClient Connect version 4.3.5.

FortiClient v5.0.10 does not support upgrading from older patch releases of version 4.3.1 to version 4.3.4.

Upgrading from FortiClient version 4.2

FortiClient v5.0.10 supports manual upgrade, upgrade through FortiGuard Distribution Servers (FDS), and upgrade through FortiManager version 4.3 from FortiClient version 4.2.

A successful software upgrade will convert and update all existing version 4.2 configurations to FortiClient v5.0.10 formats.

An Internet connection is required for both manual and FDS software upgrades.

Manual upgrade

FortiClient version 4.2 may be upgraded to FortiClient v5.0.10 by running the FortiClient v5.0.10 installation file on the client computer. The installation file can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

  Requires a support account with a valid support contract.
- FortiClient homepage: www.forticlient.com

Upgrade through FDS

FortiClient v5.0.10 is available through FDS for existing FortiClient v4.2 users. Users will receive an update notification and they may choose to accept or reject the update.

If the user accepts the update, FortiClient will proceed to complete the installation of FortiClient v5.0.10. If the update notice is rejected, the notification may be repeated at regular intervals.

Some users may have configured to *run updates automatically*. For such users, the upgrade will proceed without a prompt.

Upgrade through FortiManager

FortiClient version 4.2 client computers that are managed by FortiManager may be upgraded to FortiClient v5.0.10 by pushing the update from the FortiManager.

FortiClient v5.0.10 does not support use of FortiManager for central management. FortiGate devices running FortiOS v5.0 may be used for endpoint control.

After a successful upgrade, previously managed FortiClient systems will no longer be managed from FortiManager. The administrator should consider the impact of this on FortiClient distribution.

A software upgrade may be initiated by the administrator by manually uploading the FortiClient v5.0.10 MSI installation package to FortiManager version 4.3.

The end-user receives a notification requesting permission to proceed with the upgrade. The manual package upload allows the administrator to configure the IP address of a FortiGate that will manage the clients upon completion of the upgrade.

Push update from FortiManager to managed FortiClient agents:

1. Obtain the FortiClient v5.0.10 installation files from the Fortinet Customer Service & Support portal, https://support.fortinet.com. To download firmware images you require a support account with a valid support contract.
2. Configure the IP address of the FortiGate that will be used for managing the clients after the upgrade is completed.
3. Create a custom MSI installer file.
4. Configure *Endpoint Control* on your FortiGate device.
5. Upload the customized MSI installer file to FortiManager.
6. Distribute the MSI installer file to registered clients.

FortiClient will register to the FortiGate device after the update.

For more information on the *FortiClient Configurator GUI tool*, see “Custom FortiClient Installations” on page 109.

Downgrading to previous versions

FortiClient v5.0.10 does not support downgrading to previous FortiClient versions.

FortiClient (Mac OS X) v5.0.10 upgrade information

Please review the *FortiClient (Mac OS X) v5.0.10 Release Notes* prior to upgrading your client. The following information outlines supported upgrade paths and methods.

Upgrading from FortiClient version 5.0.0 or later

FortiClient v5.0.10 supports direct upgrade from FortiClient version 5.0.0 or later. To upgrade follow these steps:

1. In the menu-bar, shutdown FortiClient.
2. Download the online installer from either www.forticlient.com or the Customer Service & Support portal.
3. Run the online installer to upgrade to FortiClient v5.0.10.

Downgrading to previous versions

FortiClient v5.0.10 does not support downgrading to previous FortiClient versions.

Uninstall FortiClient

To uninstall FortiClient v5.0.10, use the *Application* > *FortiClient* > *Uninstaller application.*

Dragging and dropping the FortiClient icon to the trash folder will not remove all FortiClient components. Please use the FortiClient Uninstaller application located in the Applications folder.

Appendix A: Deployment Scenarios

Basic FortiClient Profile

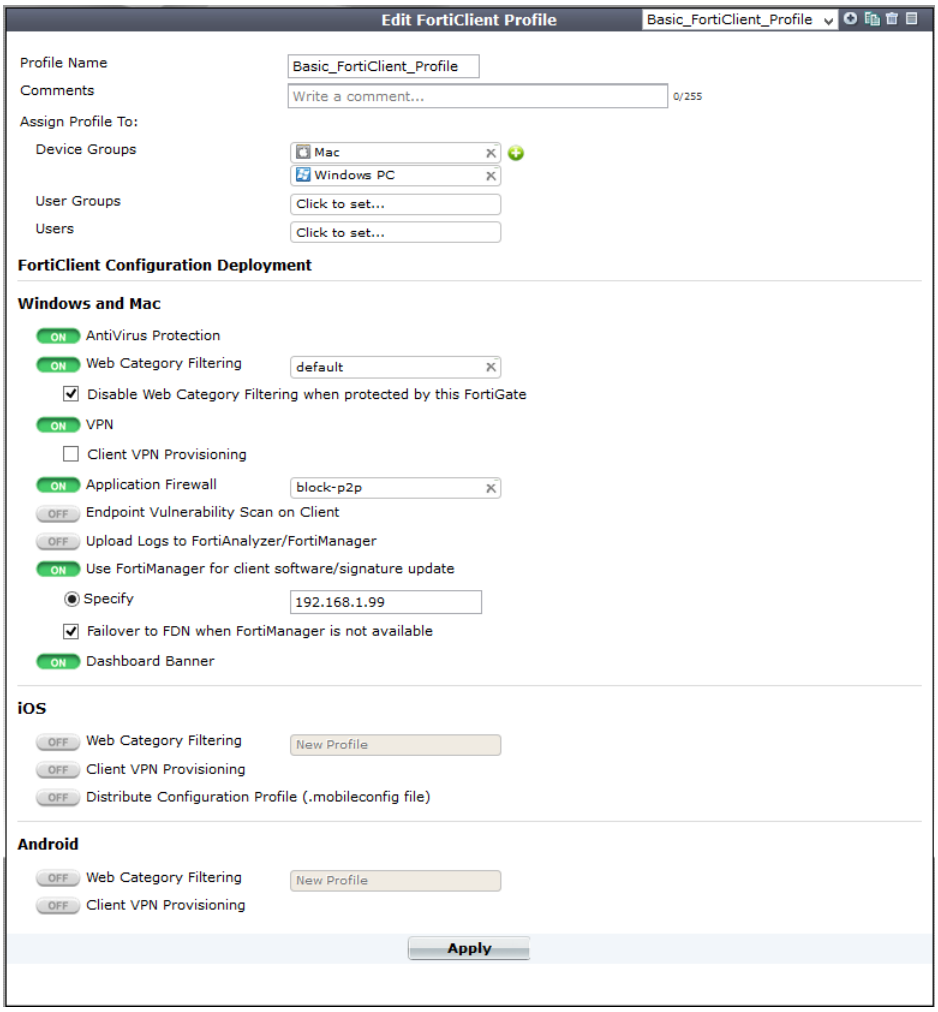
In this scenario, you want to configure all FortiClient Profile settings in the FortiGate Web-based Manager. When clients register to the FortiGate, they will receive the settings configured in the FortiClient Profile. You can configure the default profile, or create a new profile. When creating a new profile, you have additional options to specify device groups, user groups, and users.

Create a basic FortiClient Profile:

1. In the FortiGate Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. You can either select the default FortiClient Profile or select *Create New* in the toolbar. The default FortiClient Profile does not include the *Device Groups, User Groups,* and *Users* settings.

   The *Edit Endpoint Profile* page opens.

Figure 104: Basic FortiClient Profile



2. Set the device groups, user groups, user settings, and other FortiClient Profile settings as required and select *Apply* to save the FortiClient Profile changes.

Advanced FortiClient Profile (Full XML configuration)

In this scenario, you have created a custom XML configuration file. The custom file includes all settings required by the client at the time of deployment. When the client registers to the FortiGate, you want to ensure that the client receives the full XML configuration. For future configuration changes you can use the "Advanced FortiClient Profile (Partial XML configuration)" procedure.

The buffer size in the FortiClient Profile is 32kB. Depending on the size of the FortiClient XML configuration file you may not be able to deploy the full XML configuration file in the FortiClient Profile. Alternatively, you can create a custom installation file with the repackager tool and push a partial XML configuration. For more information, see "Advanced FortiClient Profile (Partial XML configuration)".

To reduce the size of the FortiClient XML configuration file, you can delete all help text found within the `<!-- .... -->` comment tags.

Create an advanced FortiClient Profile with the full XML configuration provisioned:

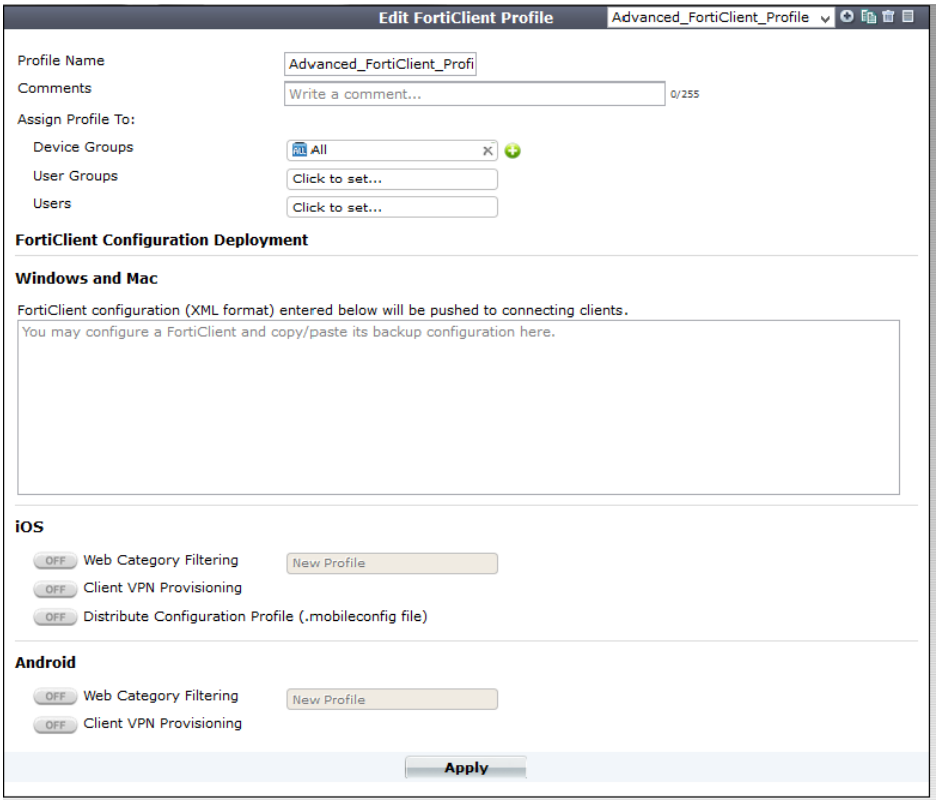
1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
  end
end
```

2. In the FortiGate Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar.

   The *Edit FortiClient Profile* page opens.

Figure 105: Advanced Endpoint Profile



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the FortiClient XML configuration file into the XML text field in the FortiClient Profile.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required, and select *Apply* to save the FortiClient Profile changes. In the future, if you need to update the FortiClient configuration follow the procedure in "Advanced FortiClient Profile (Partial XML configuration)".

Advanced FortiClient Profile (Partial XML configuration)

In this scenario, you have created a custom XML configuration file and you have created a custom FortiClient installation file using the repackaging tool. The custom XML configuration file includes most settings required by the client at the time of deployment. Due to the 32kB buffer size limitation, you are not able to follow "Advanced FortiClient Profile (Full XML configuration)" procedure.

When the client registers to the FortiGate, you want to ensure that the client receives the partial XML configuration. The partial configuration will be merged with the existing XML configuration.

Create an advanced FortiClient Profile with the partial XML configuration provisioned:

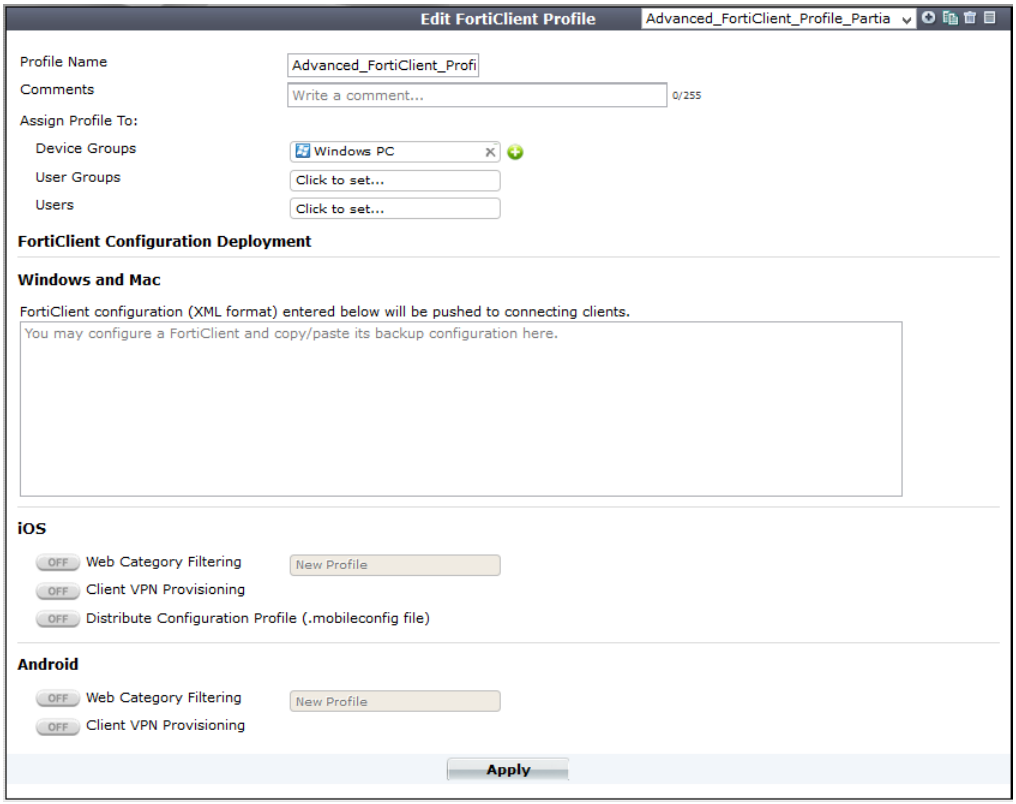
1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
  end
end
```

2. In the FortiGate Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar.

   The *Edit FortiClient Profile* page opens.

Figure 106: Advanced FortiClient Profile



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the following lines directly from the source code editor into the XML text field in the FortiClient profile:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
  .......
</forticlient_configuration>
```

   By setting the `<partial_configuration>` statement to `1`, the XML configuration will be merged into the existing XML configuration.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required and select *Apply* to save the FortiClient Profile changes. In the future if you need to update the FortiClient configuration follow the procedure in "Advanced FortiClient Profile (Partial XML configuration)".

Advanced VPN Provisioning FortiClient Profile

In this scenario, you want to provision multiple XML VPN configurations while setting the other FortiClient Profile settings in the FortiGate Web-based Manager. As the current buffer size in the CLI is 32kB, your FortiClient XML configuration may be too large to deploy using the regular advanced FortiClient Profile. You can use the repackaging tool to configure settings which are not available in the FortiClient Profile page by including the FortiClient XML configuration file in the installation

Create an advanced FortiClient Profile with XML VPN configurations:

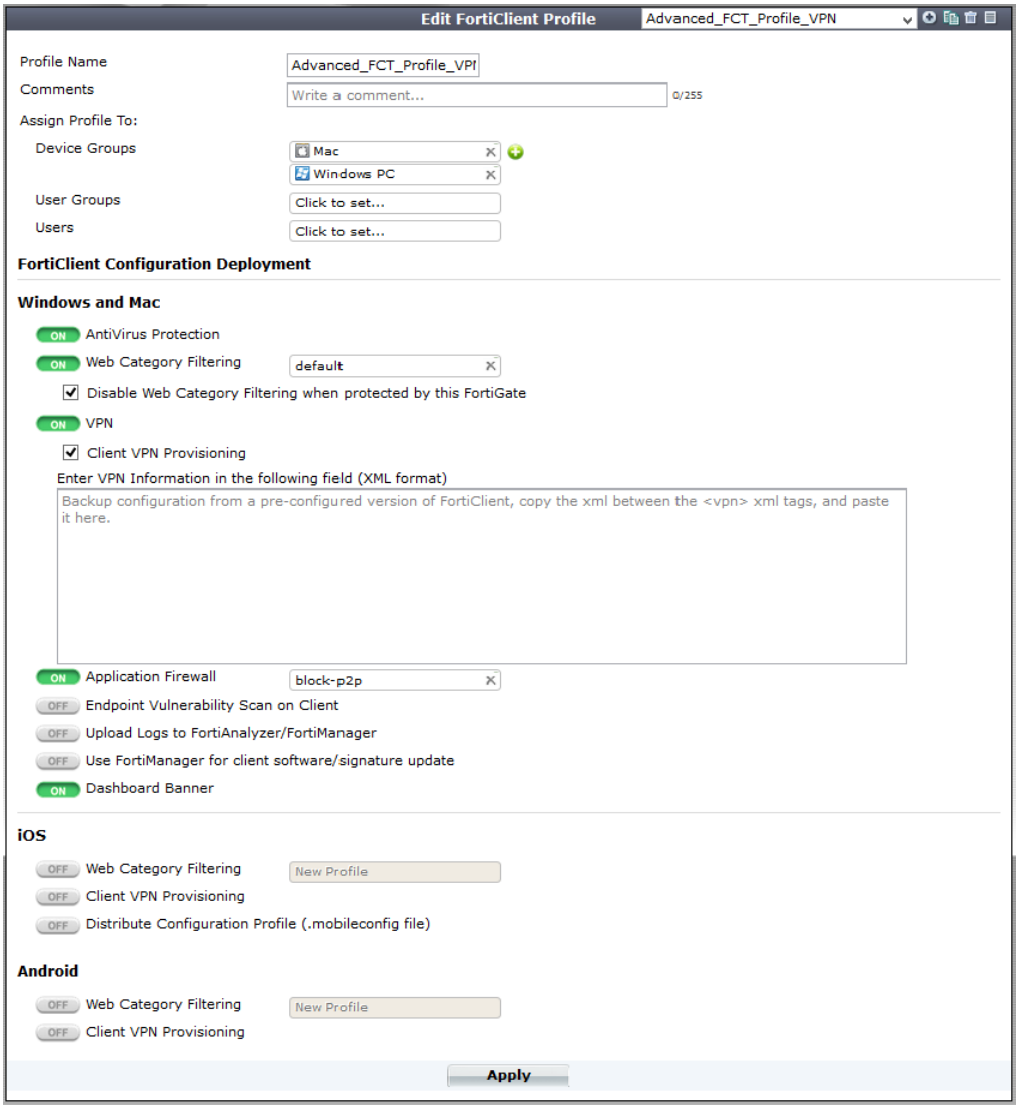
1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-vpn-provisioning enable
    set forticlient-advanced-vpn enable
  end
end
```

2. In the FortiGate Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar.

   The *Edit FortiClient Profile* page opens.

Figure 107: Advanced VPN FortiClient Profile



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste all information from the <vpn> comment tag to the </vpn> comment tag directly from the source code editor into the XML text field in the endpoint profile.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-vpn-buffer` command.

4. Set the device groups, user groups, user settings, and other FortiClient Profile settings as required and select *Apply* to save the FortiClient Profile changes.

Advanced FortiClient Profile (No settings provisioned)

In this scenario, you have created a custom installation file using the repackager tool. The custom file includes all settings required by the client at the time of deployment. When the client registers to the FortiGate, you want to ensure that no settings are pushed to the client and the XML configuration remains intact.

When changes are required you can push a partial configuration to the clients with the specific XML configuration changes.

Create an advanced FortiClient Profile with no settings provisioned:

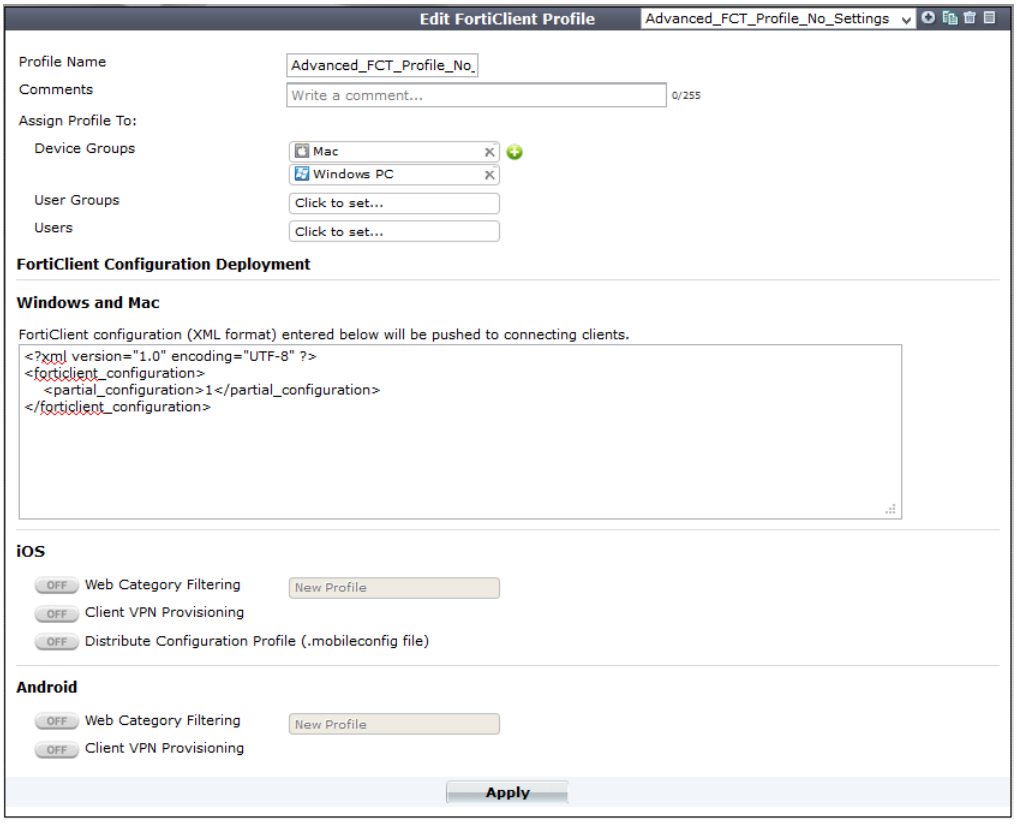
1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
  edit <profile_name>
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
  end
end
```

2. In the FortiGate Web-based Manager, go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar.

   The *Edit FortiClient Profile* page opens.

Figure 108: Advanced FortiClient Profile



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the following lines directly from the source code editor into the XML text field in the FortiClient profile:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
</forticlient_configuration>
```

By setting the `<partial_configuration>` statement to `1`, the XML configuration will be merged into the existing XML configuration. Since no other XML statements are included, no changes will be made to the XML configuration on the client.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required and select *Apply* to save the FortiClient Profile changes. In the future if you need to update the FortiClient configuration follow the procedure in "Advanced FortiClient Profile (Partial XML configuration)".

Using Active Directory Groups

Some organizations may choose to deploy different FortiClient profiles to different user groups. FortiOS is able to send different FortiClient profiles based on the AD group of the user. This requires use of the FortiAuthenticator.

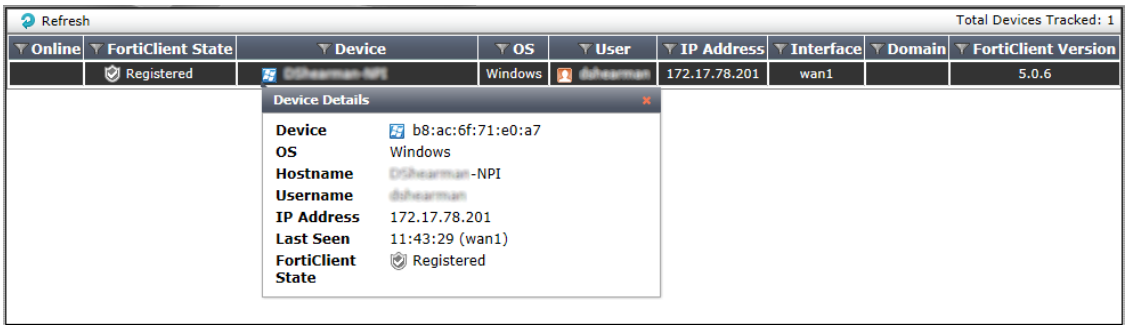
No special configuration is required on FortiClient.

Monitoring registered users

An administrator can monitor managed FortiClient users. When the client successfully registers to the FortiGate, the client can be monitored on the FortiGate.

In the FortiOS Web-based Manager, all registered clients can be observed on the *User & Device* > *Monitor* > *FortiClient* page.

Figure 109: Monitor registered clients



Either of the following FortiOS CLI commands will list all registered clients:

- `diagnose endpoint registration list`, or
- `diagnose endpoint record-list`.

Customizing FortiClient using XML settings

FortiClient configurations can be customized at the XML level. For more information, see the FortiClient v5.0.10 XML Reference.

Silent registration

You may want to configure FortiClient to silently register to FortiGate without any user interaction. When configured, the user will not be prompted to register to a FortiGate. The following XML element can be used to enable this:

```
<forticlient_configuration>
  <endpoint_control>
    <silent_registration>1</silent_registration>
  </endpoint_control>
</forticlient_configuration>
```

Locked FortiClient settings

End-users with administrator permission on their Windows system have access to the FortiClient settings page. If this is not desired, it can be locked with a password from the FortiGate. The following FortiOS Command Line Interface (CLI) command, when included, requires that any client registered to the FortiGate to provide the password before they can access the settings page.

```
config endpoint-control profile
  edit "fmgr"
    config forticlient-winmac-settings
      ...
      set forticlient-settings-lock disable
      set forticlient-settings-lock-passwd <password>
      ...
      end
    ...
    next
  end
```

Disable unregistration

With silent endpoint control registration enabled, a user could unregister after FortiClient has registered to the FortiGate. The capability to unregister can be disabled using the following XML element:

```
<forticlient_configuration>
  <endpoint_control>
    <disable_unregister>0</disable_unregister>
  </endpoint_control>
</forticlient_configuration>
```

Putting it together

Here is a sample complete FortiClient v5.0.10 XML configuration file with the capabilities discussed above:

```
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
  <endpoint_control>
    <enabled>1</enabled>
    <disable_unregister>1</disable_unregister>
    <silent_registration>1</silent_registration>
    <fortigates>
      <fortigate>
        <serial_number />
        <name />
        <registration_password>un9r3Ak@b!e</registration_password>
        <addresses>newyork.example.com</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The FortiGate that is registered to is listed in the `<fortigates>` element. The `<registration_password>` element is required if the endpoint control configuration on the FortiOS requires one. This can be exported as an encrypted file from a registered FortiClient.

The configuration provided above is not the full FortiClient configuration file. Thus, the `<partial_configuration>` element is set to `1`.

Appendix B: Using the FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API. The API can be used with IPsec VPN only. SSL VPN is currently not supported.

This chapter contains the following sections:

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - configured tunnel list
  - active tunnel name
  - connected or not
  - idle or not
  - remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN Automation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values.

Table 7: Methods

`Connect(bstrTunnelName As String)`	Open the named VPN tunnel. This connection must already be configured in your FortiClient application.
`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetPolicy pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)`	Command is deprecated in FortiClient v5.0.

Table 7: Methods (continued)

`Connect(bstrTunnelName As String)`	Open the named VPN tunnel. This connection must already be configured in your FortiClient application.
`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether keylife time (per seconds) or data (per KB) are significant depends on the detailed settings in the FortiClient application.
`MakeSystemPolicyCompliant()`	Command is deprecated in FortiClient v5.0.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: User name, Password True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.

Table 8: Functions

`GetActiveTunnel() As String`	Retrieve the name of the active connection.
`GetTunnelList()`	Retrieve the list of all connections configured in the FortiClient application.
`IsConnected (bstrTunnelName As String) As Boolean`	Return True if the named connection is up.
`IsIdle (bstrTunnelName As String) As Boolean`	Return True if the named connection is idle.

Table 9: Events

`OnConnect(bstrTunnelName As String)`	Connection established.
`OnDisconnect(bstrTunnelName As String)`	Connection disconnected.
`OnIdle(bstrTunnelName As String)`	Connection idle.
`OnOutOfCompliance(bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

Appendix C: FortiClient FIPS Image

Introduction

FortiClient v5.0.10 includes an Federal Information Protection Standards (FIPS) 140-2 Level 2 supported installation file for both 32-bit and 64-bit systems. When installing the FIPS image, only Remote Access (VPN) is installed. No other modules are installed and central endpoint management is not available.

Summary of FIPS features

FortiClient FIPS has several differences compared to the non-FIPS image. The main feature changes include:

- use of FortiTRNG entropy token;
- self-tests;
- minimum certificate key length;
- MD5 and DES are disabled.

Supported platforms

FortiClient FIPS supports Microsoft Windows 7 x86, x64 and newer versions. Microsoft Windows Vista and Windows XP are not supported. Microsoft Windows Servers have not been tested.

At this time, a FortiClient FIPS installation file is not available for Mac OS X, Android OS or iOS.

Installing FortiClient FIPS

FortiClient FIPS requires use of the FIPS build. Installation follows the usual FortiClient process, with only the following differences:

- a license key is required at the time of installation;
- only the Remote Access (VPN) module is installed;
- upgrade from any previous FortiClient installation is not supported;
- cannot switch from non-FIPS build to FIPS build, or the other way around;
- there is no signature update right after the initial installation (since the Antivirus feature is not installed).

Custom FortiClient configurations can be created using FortiClient Configurator to create an installer.

Licensing

FortiClient FIPS requires each individual installation to be licensed. A license key must be provided at the time of installation.

The license is validated in two phases:

- the FortiClient installer checks that the license key is a valid key;
- the installer then sends the license key to Fortinet for validation and to check the seat limits.

If validation fails in either step, installation cannot proceed.

FIPS operation

FortiClient VPN uses cryptography to protect the data exchanged with VPN servers. The FIPS 140-2 standard places restrictions on some of the cryptography tools and techniques that can be used, and requires some others to be offered.

FortiTRNG entropy token

FortiClient FIPS offers the option to use FortiTRNG (Fortinet True Random Number Generator) to create random numbers for use in cryptography functions. This is a USB device that is inserted into a computer USB port during usage.

There are three possible states:

- enabled
- disabled
- dynamic

When FortiTRNG is enabled, entropy is generated using the FortiTRNG token for seeding. If disabled, FortiTRNG is not used for seeding. Instead FortiClient will use its existing method of generating seeds. The dynamic option indicates to use the FortiTRNG for seeding when available (inserted into the computer), and use the in-built alternative method otherwise.

FortiTRNG can be enabled or disabled using the XML configuration:

```
<forticlient_configuration>
  <cryptography>
    <entropy_token_mode>0</entropy_token_mode>
  </cryptography>
</forticlient_configuration>
```

where `<entropy_token_mode>` is:

```
0 - disable FortiTRNG
1 - enable FortiTRNG
2 - dynamic (use FortiTRNG if present)
```

Reseeding will occur every 1440 minutes (one day) by default. The reseeding interval can be changed using the following FortiClient XML configuration element:

```
<forticlient_configuration>
  <cryptography>
    <drbg_reseed_minutes>0</drbg_reseed_minutes>
  </cryptography>
</forticlient_configuration>
```

Reseeding is required only when FortiTRNG is enabled. Reseeding is not done when the entropy token mode is set to `dynamic` or `disabled`. Similarly, reseeding is disabled if the `<drbg_reseed_minutes>` is set to `0`.

FortiClient FIPS will enter FIPS error mode if the FortiTRNG is enabled but the FortiTRNG token is not present at reseed time.

Cryptography changes

The following changes affect cryptography functions:

- IPsec VPN IKE supports Diffie-Hellman (DH) group of up to 14. The non-FIPS image also supports a DH group of 14.
- MD5 and DES are both disabled
- TLS 1.0 is the minimum cipher that could be used. SSLv3 or older are not supported.

Index

D

E

F

R

S

T

U